eeeeeeeeeeeeeeeee

3Com® Switch 4500 Family
Command Reference Guide

Switch 4500 26-Port
Switch 4500 50-Port
Switch 4500 PWR 26-Port
Switch 4500 PWR 50-Port

www.3Com.com
Part No. 10015729, Rev. AA
Published: January 2007

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

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com and the 3Com logo are registered trademarks of 3Com Corporation.

Cisco is a registered trademark of Cisco Systems, Inc.

Funk RADIUS is a registered trademark of Funk Software, Inc.

Aegis is a registered trademark of Aegis Group PLC.

Intel and Pentium are registered trademarks of Intel Corporation. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Novell and NetWare are registered trademarks of Novell, Inc. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

IEEE and 802 are registered trademarks of the Institute of Electrical and Electronics Engineers, Inc.

All other company and product names may be trademarks of the respective companies with which they are associated.

ENVIRONMENTAL STATEMENT

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

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

Conserving energy, materials and natural resources in all operations.

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

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

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

Improving our environmental record on a continual basis.

End of Life Statement

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

Regulated Materials Statement

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

Environmental Statement about the Documentation

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

CONTENTS

ALPHABETICAL LISTING OF COMMANDS

About This Guide

This guide provides all the information you need to use the configuration commands supported by version 3.0.x software on the 3Com® Switch 4500.

About This Software Version

The software in the Switch 4500 is a subset of that used in some other 3Com products. Depending on the capabilities of your hardware platform, some commands described in this guide may not be available on your Switch, although the unavailable commands may still display on the command line interface (CLI). If you try to use an unavailable command, an error message displays.

CAUTION: *Any command that displays on the CLI, but is not described in this guide, is not supported in version 3.0.x software. 3Com only supports the commands described in this guide. Other commands may result in the loss of data, and are entered at the user's risk.*

How This Guide is Organized

The Switch 4500 Command Reference Guide consists of the following chapters:

- **Using System Access Commands** — Introduces the commands used for accessing the Switch 4500.
- **Using Port Commands** — Introduces the commands used for configuring Ethernet port and link aggregation.
- **Using VLAN Commands** — Introduces the commands used for configuring VLANs.
- **Using Power over Ethernet (PoE) Commands** — Introduces the commands used for configuring PoE.
- **Using Network Protocol Commands** — Introduces the commands used for configuring network protocols.
- **Using Routing Protocol Commands** — Introduces the commands used for configuring routing protocols.
- **Using Multicast Protocol Commands** — Introduces the commands used for configuring multicast protocols.
- **Using QoS and ACL Commands** — Introduces the commands used for configuring QoS/ACL.
- **Using STP Commands** — Introduces the commands used for configuring STP.
- **Using AAA and RADIUS Commands** — Introduces the commands used for configuring 802.1x, AAA and RADIUS.
- **Using Reliability Commands** — Introduces the commands used for configuring VRRP.

- **Using System Management Commands** — Introduces the commands used for system management and maintenance.

Intended Readership

The guide is intended for the following readers:

- Network administrators
- Network engineers
- Users who are familiar with the basics of networking

Conventions

This guide uses the following conventions:

Table 1 Icons

Icon	Notice Type	Description
	Information note	Information that describes important features or instructions.
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device.
	Warning	Information that alerts you to potential personal injury.

Table 2 Text conventions

Convention	Description
`Screen displays`	This typeface represents text as it appears on the screen.
Keyboard key names	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+), for example: Press Ctrl+Alt+Del
The words "enter" and "type"	When you see the word "enter" in this guide, you must type something, and then press Return or Enter. Do not press Return or Enter when an instruction simply says "type."
`Fixed command text`	This typeface indicates the fixed part of a command text. You must type the command, or this part of the command, exactly as shown, and press *Return* or *Enter* when you are ready to enter the command. Example: The command **`display history-command`** must be entered exactly as shown.
`Variable command text`	This typeface indicates the variable part of a command text. You must type a value here, and press *Return* or *Enter* when you are ready to enter the command. Example: in the command **`super`** ***`level`*** , a value in the range 0 to 3 must be entered in the position indicated by ***`level`***
{ x | y | ... }	Alternative items, one of which must be entered, are grouped in braces and separated by vertical bars. You must select and enter one of the items. Example: in the command **`flow-control {hardware`** | **`none`** | **`software}`**, the braces and the vertical bars combined indicate that you must enter one of the parameters. Enter either **`hardware`**, or **`none`**, or **`software`**.

Table 2 Text conventions

[ ]	Items shown in square brackets [ ] are optional. Example 1: in the command **`display users [all]`**, the square brackets indicate that the parameter **`all`** is optional. You can enter the command with or without this parameter. Example 2: in the command **`user-interface`** [**`type`**] **`first-number`** [**`last-number`**] the square brackets indicate that the parameters [**`type`**] and [**`last-number`**] are both optional. You can enter a value in place of one, both or neither of these parameters. Alternative items, one of which can optionally be entered, are grouped in square brackets and separated by vertical bars. Example 3: in the command **`header [shell`** | **`incoming`** | **`login] text`**, the square brackets indicate that the parameters **`shell`**, **`incoming`** and **`login`** are all optional. The vertical bars indicate that only one of the parameters is allowed.

Related Documentation

The *3Com Switch 4500 Getting Started Guide* provides information about installation.

The *3Com Switch 4500 Configuration Guide* provides information about configuring your network using the commands described in this guide.

1 USING SYSTEM ACCESS COMMANDS

This chapter describes how to use the following commands:

Logging in Commands

Logging in Commands

This section describes the commands that you can use to configure system access and system security.

authentication-mode

Syntax

authentication-mode { password | scheme | none }

View

User interface view

Parameter

password: Requires local authentication of password at log in.

scheme: Requires local or remote authentication of username and password at log in.

none: Allows users to log in without username or password.

Description

This command configures the authentication method for a user at log in.

Use the command **authentication-mode password** to prompt a user for local password authentication at login. To set the password, use **set authentication password**.

Use the command **authentication-mode scheme** to prompt a user to provide local or remote user name and password authentication at login. The type of the authentication depends on your network configuration. For further information, see "AAA and RADIUS".

Use the command **authentication-mode none** to allow a user to log in without username or password authentication.

By default, users logging in using the console port do not need to pass any terminal authentication. Users logging in via modem or Telnet are required to provide password authentication when they log in.

Example

To configure local password authentication, enter the following command:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]user-interface aux 0
[4500-ui-aux0]authentication-mode password
```

auto-execute command

Syntax

auto-execute command *text*

undo auto-execute command

View

User Interface View

Parameter

text: Specifies the command to be run automatically.

Description

Enter **auto-execute command *text*** to configure the Switch to automatically run a specified command. When the user logs in, the command will be executed automatically. This command is usually used to configure the **telnet** command on the terminal, which will connect the user to a designated device automatically.

Enter **undo auto-execute command** to cancel the auto-execute command so the command is not run automatically.

By default, auto-execute is disabled.

CAUTION*: If you execute this command, the user-interface can no longer be used to perform routine configurations on the local system. Ensure that you can log in to the system in some other way to cancel the configuration, before you configure the* **auto-execute command** *and save the configuration.*

Example

To configure the Switch to automatically Telnet to device 10.110.100.1 after the user logs in via VTY 0, enter the following command:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]user-interface vty 0
[4500-ui-vty0]auto-execute command telnet 10.110.100.1
```

command-privilege level

Syntax

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

undo command-privilege view *view command*

View

System View

Parameter

level: Enter the command level you want to assign to this command, ranging from 0 to 3.

view: Enter the name of the view that contains the command. This can be any of the views supported by the Switch.

command: Enter the command to be configured.

Description

Use the **command-privilege level** command to configure the priority level assigned to any command within a selected view.

The command levels are, from lowest to highest:

- **0** – Visit
- **1** – Monitoring
- **2** – System
- **3** – Management

When the user logs into the Switch, the commands used depends on the user level settings and the command level settings on the user interface. The two types of settings may differ as follows:

- If AAA/RADIUS authentication is used, the commands the user can access are determined by the user level settings. For example, if a user is set to level 3 and the command level on the VTY 0 user interface is level 1, the user can only user the commands of level 3 or lower when logging into the Switch from the VTY interface.
- If RSA public key authentication is used, the commands the user can access are determined by the command level settings on the user interface.

By default:

- ping, tracert, and telnet are at level 0
- display and debugging are at level 1
- all configuration commands are at system level 2
- FTP, XMODEM, TFTP and commands for file system operations are at level 3

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

Example

To configure the precedence of the command 'interface' as 0, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]command-privilege level 0 view system interface
```

databits

Syntax

databits { 7 | 8 }

undo databits

View

User interface view

Parameter

7 – Sets the data bits to 7.

8 – Sets the data bits to 8.

Description

Use the **databits** command to configure the data bits for the AUX (Console) port to either **7** or **8**. By default, the value is **8**. Use the **undo databits** command to restore the default value (8).

This command can only be performed in the AUX user interface view.

Example

To configure the data bits of the AUX (Console) port to 7 bits, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]user-interface aux 0
[4500-ui-aux0]databits 7
```

display history-command

Syntax

display history-command

View

All views

Parameter

None

Description

Use the **display history-command** command to view the commands previously entered during this login session, up to a specified maximum.

To set the maximum number of commands to display, see **history-command max-size**.

Example

To display previously entered commands, enter the following.

```
<4500>display history-command
```

The commands display on screen.

display user-interface

Syntax

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

View

All views

Parameter

type number: Enter the type and number of the user interface you want to display details on, for example VTY 3.

number: Enter the index number of the user interface you want to display details on.

summary: Display the summary of a user interface.

Description

Use the **display user-interface** command to view information on a user interface. You can choose to access this information by user interface type and type number, or by user interface index number. The information displayed is the same whichever access method you use.

This command without the **summary** parameter displays user interface type, absolute/relative index, transmission speed, priority, authentication methods, and physical location. This command with the **summary** parameter displays one user interface in use with user interface name and other user interface information.

Example

To display information on a user interface with an index number of 0, enter the following.

```
<4500>display user-interface aux 0
```

The information is displayed in the following format:

```
Idx  Type     Tx/Rx      Modem Privi Auth  Int
  0    AUX 0    19200      -     3     P     -

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

Table 3 Output description of the **display user-interface** command

Field	Description
+	Indicates that the user interface is in use
F	Current user interface is in use and working in asynchronous mode
Idx	Displays the index number of the user interface
Type	Displays the type and type number of the user interface
Tx/Rx	Displays the user interface speed
Modem	Displays the modem operation mode
Privi	Indicates the command level that can be accessed from this user interface
Auth	Indicates the user interface authentication method
Int	Indicates the physical location of the user interface

Display the summary information of user interface 0.

```
<4500>display user-interface 0 summary
0: U
```

```
1 character mode users.      (U)
1 total UIs in use.
UI's name: aux0
```

Table 4 Output Description of the **display user-interface summary** Command

Field	Description
0: U	User interface type
1 character mode users	One type of user interface
1 total UIs in use	The total number of user interfaces in use
UI's name	User interface name

display users

Syntax

display users [all]

View

All views

Parameter

all: Enter to display information on all user interfaces.

Description

Use the **display users** command to view information on the current user interface. Use the **display users all** command to view the information on all user interfaces.

Example

To display information on the current user interface, enter the following

```
[4500]display users
```

The information displays in the following format:

```
     UI      Delay   Type    IPaddress  Username   Userlevel
F 0 AUX 0    00:00:00             3
```

The categories of information displayed are as follows:

Table 5 Output description of the **display users** command

Field	Description
F	Indicates that the user interface is in use and is working in asynchronous mode
UI	Number of the first list is the absolute number of user interface.
	Number of the second list is the relative number of user interface
Delay	Indicates the interval from the latest input until now, in seconds.
Type	Indicates the user interface type.
IPaddress	Displays initial connection location, namely the host IP address of the incoming connection.
Username	Display the login name of the user who is using this interface
Userlevel	Display the level of the user using this user interface

flow-control

Syntax

flow-control { hardware | none | software }

undo flow-control

View

User interface view

Parameter

hardware: Enter to set hardware flow control.

none: Enter to set no flow control.

software: Enter to set software flow control.

Description

Use the **flow-control** command to configure the flow control mode on the AUX (Console) port to hardware, software or none. Use the **undo flow-control** command to restore the default flow control mode (no flow control).

This command can only be performed in the AUX user interface view.

Example

To configure software flow control on the AUX (Console) port, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]user-interface aux 0
[4500-ui-aux0]flow-control software
```

free user-interface

Syntax

free user-interface { *type* | *number* }

View

User view

Parameter

type: Enter the type and type number of the user interface to be reset.

number: Enter the index number of the user interface to be reset.

Description

Use this command to reset a specified user interface to its default settings. The user interface will be disconnected after the reset.

Use **free user-interface *type*** to reset the interface with the specified type and type number to its default settings. Use **free user-interface *number*** to reset the interface with the specified index number to its default settings.

You cannot use this command on the current user interface.

Example

To reset user interface AUX 1 from another user interface on the Switch, enter the following:

```
<4500>free user-interface aux 1
```

After the command is executed, user interface AUX 1 is disconnected. When you next log in using user interface AUX 1, it opens using the default settings.

header

Syntax

header { shell | **incoming** | **login }** ***text***

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

View

System view

Parameter

login: Login information in case of authentication. It is displayed before the user is prompted to enter user name and password.

shell: User conversation established header, the information output after user conversation has been established. If authentication is required, it is prompted after the user passes authentication.

incoming: Login header, the information output after a Modem user logs in. If authentication is required, it is prompted after the user passes authentication. In this case, no shell information is output.

text: Specifies the title text. If you do not choose any keyword in the command, the system displays the login information by default. The system supports two types of input mode: you can input all the text in one line (a maximum of 256 characters, including command key word, can be entered); or you can input all the text in several lines using the <Enter> key, and more than 256 characters can be entered. The text starts and ends with the first character. After entering the last character, press the <Enter> key to exit the interactive process.

Description

Use the **header** command to configure the system to display a header during user log in. Use the **undo header { shell** | **incoming** | **login }** command to delete the specified header.

When the user logs in, and a connection is activated, the **login** header displays. After the user successfully logs in, the **shell** header displays.

The first characters in the text are regarded as the start and stop characters. After you type in the stop character, the system will exit the header command automatically.

If you do not want to use the control characters, you can type in text with the same characters at the beginning and end, and press *Enter*.

If you press <Enter> after typing any of the three keywords shell, login and incoming in the command, then what you type after the word header is the contents of the login information, instead of identifying header type.

You can judge whether the initial character can be used as the header contents this way:

1. *If there is only one character in the first line and it is used as the identifier, this initial character pairs with the ending character and is not the header contents.*
2. *If there are many characters in the first line but the initial and ending characters are different, this initial character pairs with the ending character and is the header contents.*
3. *There are many characters in the first line and the initial character is identical with the ending character, this initial character is not the header contents.*

Example

Configure the header of setting up a session.

Mode 1: Input in one line

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]header shell %SHELL: Hello! Welcome%
```

The starting and ending characters must be the same, and press the <Enter> key to finish a line.

- When you log on the Switch again, the terminal displays the configured session establishment title.

```
[4500]quit
<4500>quit
Please press ENTER
SHELL: Hello! Welcome
```

The initial character "%" is not the header contents.

```
<4500>
```

Mode 2: Input in several lines

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]header shell % SHELL:
```

After you pressing the <Enter> key, the system prompts the following message:

```
Input banner text, and quit with the character '%'.
```

Go on inputting the rest text and end your input with the first letter:

```
Hello! Welcome %
```

Press the <Enter> key.

```
[4500]
```

When you log on the Switch again, the terminal displays the configured session establishment title.

```
[4500]quit
<4500>quit
Please press ENTER
%SHELL:
```

The initial character "%" is the header contents.

```
Hello! Welcome
<4500>
```

history-command max-size

Syntax

history-command max-size ***value***

undo history-command max-size

View

User interface view

Parameter

value: Enter the number of previously entered commands that you want the Switch to save.

Description

Use the command **history-command max-size** to specify the amount of previously entered commands that you want the Switch to save. Enter any value between 0 and 256. The default is 10, that is, the 10 most recently entered commands are saved. Use the **undo history-command max-size** command to restore the default value.

To display the most recently-entered commands, up to the specified maximum, use the command **display history-command**.

Example

To set the history buffer to 20, that is to save the 20 most recently-entered commands, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]user-interface aux 0
[4500-ui-aux0]history-command max-size 20
```

idle-timeout

Syntax

idle-timeout ***minutes*** **[** ***seconds*** **]**

undo idle-timeout

View

User interface view

Parameter

minutes: Enter the number of minutes you want to allow a user interface to remain idle before it is disconnected. This can be in the range 0 to 35791.

seconds: Enter the number of seconds in addition to the number of minutes. Optional.

Description

Use the **idle-timeout** command to configure the amount of time you want to allow a user interface to remain idle before it is disconnected. Use the **undo idle-timeout** command to restore the default idle-timeout. By default, idle-timeout is set to 10 minutes.

To disable idle timeout, set the **idle-timeout** value to **0**.

Example

To configure the timeout value to 1 minute on the AUX user interface, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]user-interface aux 0
[4500-ui-aux0]idle-timeout 1
```

language-mode

Syntax

language-mode { chinese | english }

View

User View

Parameter

chinese: Sets the language of the command line interface to Chinese.

english: Sets the language of the command line interface to English.

Description

Use the **language-mode** command to choose the language of the command line interface. By default, the command line interface is set to English.

Example

To change the command line interface from English to Chinese, enter the following:

```
<4500-ui-aux0>language-mode chinese
```

lock

Syntax

lock

View

User View

Parameter

None

Description

Use the **lock** command to lock the current user interface and prevent unauthorized users from accessing it. An authorized user must enter a valid password to access the interface.

Example

To lock the current user interface, enter the following:

```
<4500>lock
Password: xxxx
Again: xxxx
```

parity

Syntax

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

undo parity

View

User Interface View

Parameter

even: Sets the Switch to even parity.

mark: Sets the Switch to mark parity (1)

none: Sets the Switch to perform no parity checking.

odd: Sets the Switch to odd parity.

space: Sets the Switch to zero parity (0)

Description

Use the **parity** command to configure the parity mode on the AUX (Console) port. Use the **undo parity** command to restore the default parity mode (no parity checking).

This command can only be performed in the AUX user interface view.

Example

To set mark parity on the AUX (Console) port, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]user-interface aux 0
[4500-ui-aux0]parity mark
```

protocol inbound

Syntax

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

View

VTY user interface view

Parameter

all: Supports both Telnet and SSH protocols.

ssh: Supports only SSH protocol.

telnet: Supports only Telnet protocol.

Description

Use the **protocol inbound** command to configure the protocols supported by a designated user interface.

By default, the user interface supports Telnet and SSH protocol.

For the related commands, see **user-interface vty**.

Example

Configure SSH protocol supported by VTY0 user interface.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]user-interface vty 0
[4500-ui-vty0]protocol inbound ssh
```

quit

Syntax

quit

View

All views

Parameter

None

Description

Use the **quit** command to exit from the current view to the next highest view. If the current view is user view, this command quits the system.

There are three levels of view, which are, from high to low:

- user view
- system view
- menu views, for example VLAN view, Ethernet port view, and so on.

Related commands: **return**, **system-view**.

Example

To return to user view from system view, enter the following:

```
[4500]quit
<4500>
```

return

Syntax

return

View

System view or higher

Parameter

None

Description

Use the **return** command to return to user view from any other view.

Ctrl+Z performs the same function as the **return** *command.*

To return to the next highest level of view, use **quit**.

Example

To return to user view from any other view (the example below shows the command entered from the system view), enter the following.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]return
<4500>
```

screen-length

Syntax

screen-length ***screen-length***
undo screen-length

View

User interface view

Parameter

screen-length: Enter the maximum number of information lines that you want to display on a terminal screen, ranging from 0 to 512. The default is 24.

Description

Use the command **screen-length** to configure how many information lines (maximum) will be displayed on the screen of a terminal. Use the command **undo screen-length** to restore the default of 24 lines.

To disable this function, that is to allow an unlimited number of information lines, enter the parameter as **0**.

Example

To configure a terminal to display 20 lines of information, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]user-interface aux 0
[4500-ui-aux0]screen-length 20
```

send

Syntax

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

View

User view

Parameter

all: Sends a message to all user interfaces.

type: Enter the type and type number of the user interface that you want to send a message to.

number: Enter the absolute/relative number of the interface that you want to send a message to.

Description

Use the **send** command to send messages to other user interfaces.

Example

To send a message to all the user interfaces, enter the following:

```
<4500>send all
```

service-type

Syntax

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

View

Local-user View

Parameter

telnet: Specifies user type as Telnet.

ssh: Specifies user type as SSH.

level *level:* Specifies the level of Telnet, SSH or terminal users. The argument level is an integer in the range of 0 to 3 and defaults to 0.

ftp: Specifies user type as ftp.

ftp-directory *directory*: Specifies the directory of ftp users, directory is a character string of up to 64 characters.

lan-access: Specifies user type to lan-access, which mainly refers to Ethernet accessing users, 802.1x supplicants for example.

terminal: Authorizes the user to use the terminal service (login from the Console port).

Description

Use the command **service-type** to configure which level of command a user can access after login. Use the command **undo service-type** to restore the default level of command (level 1).

Commands are classified into four levels, as follows:

- ***0 - Visit level***. Users at this level have access to network diagnosis tools (such as ping and tracert), and the Telnet commands. A user at this level cannot save the configuration file.
- ***1 - Monitoring level***. Users at this level can perform system maintenance, service fault diagnosis, and so on. A user at this level cannot save the configuration file.
- ***2 - System level***. Users at this level can perform service configuration operations, including routing, and can enter commands that affect each network layer. Configuration level commands are used to provide direct network service to the user.
- ***3 - Management level***. Users at this level can perform basic system operations, and can use file system commands, FTP commands, TFTP commands, XModem downloading commands, user management commands and level setting commands.

Example

To allow a user **zbr** to configure commands a level 0 after login, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]local-user zbr
[4500-luser-zbr]service-type telnet level 0
```

To activate these settings, quit the system and login with the username **zbr.** Now only the commands at level 0 are listed on the terminal.

```
[4500]quit
<4500>?
User view commands:
  debugging       Debugging functions
  language-mode   Specify the language environment
  ping            Ping function
  quit            Exit from current command view
  super           Privilege current user a specified priority level
  telnet          Establish one TELNET connection
  tracert         Trace route function
  undo            Negate a command or set its default
```

set authentication password

Syntax

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

undo set authentication password

View

User interface view

Parameter

cipher: Configure to display the password in encrypted text.

simple: Configure to display the password in plain text.

password: If the authentication is in the **simple** mode, the password must be in plain text. If the authentication is in the **cipher** mode, the password can be either in encrypted text or in plain text. If a plain text password is entered when cipher mode has been selected, the password will be displayed in the configuration settings as encrypted. A plain text password is a sequential character string of no more than 16 digits, for example, 3Com918. The length of an encrypted password must be 24 digits and in encrypted text, for example, _(TT8F]Y\5SQ=^Q`MAF4<1!!.

Description

Use the **set authentication password** command to configure the password for local authentication. Use the **undo set authentication password** command to cancel local authentication password.

The password in plain text is required when performing authentication, regardless of whether the configuration is plain text or cipher text.

By default, a password is required for users connecting over Modem or Telnet. If a password has not been set, the following prompt is displayed: `Login password has not been set!`

Example

To configure the local authentication password on VTY 0 to 3Com, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]user-interface vty 0
[4500-ui-vty0]set authentication password simple 3com
```

shell

Syntax

shell

undo shell

View

User interface view

Parameter

None

Description

Use the **shell** command to enable the terminal service for a user interface. The terminal service is enabled by default. Use the **undo shell** command to disable the terminal service for a user interface.

When using the **undo shell** command, note the following points.

- For reasons of security, the **undo shell** command can only be used on user interfaces other than the AUX user interface.
- You cannot use this command on the current user interface.
- You are asked to confirm the command.

Example

To disable the terminal service on the VTY user interfaces 0 to 4, enter the following from another user interface:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]user-interface vty 0 4
[4500-ui-vty0-4]undo shell
```

speed

Syntax

speed speed-value

undo speed

View

User interface view

Parameter

speed-value: Specify the transmission rate on the AUX (Console) port in bits per second (bps). This can be any of the following values: 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 or 4096000.

The default rate is 19200 bps.

Description

Use the **speed** command to configure the transmission rate on the AUX (Console) port. Use the **undo speed** command to restore the default rate.

This command can only be performed in AUX user interface view.

Example

To configure the transmission speed on the AUX (Console) port as 9600 b/s, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]user-interface aux 0
[4500-ui-aux0]speed 9600
```

stopbits

Syntax

stopbits { 1 | 1.5 | 2 }

undo stopbits

View

User interface view

Parameter

1: Sets the stop bits to 1.

1.5: Sets the stop bits to 1.5.

2: Sets the stop bits to 2.

Description

Use the **stopbits** command to configure the stop bits on the AUX (Console) port. Use the **undo stopbits** command to restore the default stop bits (the default is 1).

This command can only be performed in AUX user interface view.

Example

To configure the stop bits to 2, enter the following from the AUX (Console) port:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]user-interface aux 0
[4500-ui-aux0]stopbits 2
```

super

Syntax

super ***level***

View

All views

Parameter

level: Enter a user level in the range 0 to 3. The default is 3.

Description

The **super** command gives a user access to a higher level than their currently assigned user level.

To ensure that only an authorized user can access the higher level, use the **super password** command to set a password for the higher level. If the user does not enter a valid password, the user level does not change.

Login users are classified into four levels that correspond to the four command levels. A user can only use commands at the levels that are equal to or lower than their user level.

Related commands: **super password**, **quit**.

Example

To change to user level 3 from the current user level.

```
<4500>super 3
Password:
```

The password prompt displays only if you set a password using the **super password** command.

super password

Syntax

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

undo super password [level *level*]

View

System View

Parameter

level: Enter a user level in the range 1 to 3. The default is 3. The password you enter is set for the specified level.

cipher: Configure to display the password in encrypted text.

simple: Configure to display the password in plain text.

password: If the authentication is in the **simple** mode, the password must be in plain text. If the authentication is in the **cipher** mode, the password can be either in encrypted text or in plain text. If a plain text password is entered when cipher mode has been selected, the password will be displayed in the configuration settings as encrypted. A plain text password is a sequential character string of no more than 16 digits, for example, 3Com918. The length of an encrypted password must be 24 digits and in encrypted text, for example, _(TT8F]Y\5SQ=^Q`MAF4<1!!.

Description

Use the **super password** command to configure the password for changing the user from a lower level to a higher level. To prevent unauthorized users from illegal intrusion, user ID authentication is performed when users switch from a lower level to a higher level. For the sake of confidentiality, on the screen the user cannot see the password that he entered. The user has three chances to input valid password, and then switch to the higher level. Otherwise, the original user level will remain unchanged. Use the **undo super password** command to cancel the password settings.

The password in plain text is required when performing authentication, regardless of whether the configuration is plain text or encrypted text.

Example

To set the password for level 3 to **zbr**, type the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]super password level 3 simple zbr
```

sysname

Syntax

sysname ***text***

undo sysname

View

System View

Parameter

text: Enter the host name of the Switch. The host name must be no more than 30 characters long. The default is 4500.

Description

Use the **sysname** command to configure the host name of the Switch. Use the **undo sysname** command to restore the host name to the default of 4500.

Changing the hostname of the Ethernet switch will affect the prompt of command line interface. For example, if the hostname of the Ethernet switch is MyHost, the prompt in user view will be <MyHost>.

Example

To configure the hostname of the Switch to 3Com, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]sysname 3Com
[3Com]
```

system-view

Syntax

system-view

View

User view

Parameter

None

Description

Enter **system-view** to enter the system view from the user view.

Related commands: **quit**, **return**.

Example

To enter system view from user view, enter the following:

```
<4500>system-view
System view: return to User View with Ctrl+Z.
[4500]
```

telnet

Syntax

telnet { ***hostname*** | ***ip_address*** } [***service_port***]

View

User view

Parameter

hostname: Enter the host name of the remote Switch. It is configured using the **ip host** command.

ip_address: Enter the IP address or the host name of the remote Switch. If you enter the host name, the Switch must be set to static resolution.

service_port: Designates the management port on the remote Switch, in the range 0 to 65535. Optional.

Description

Use the **telnet** command to log in to another Ethernet switch from the current switch via Telnet for remote management. To terminate the Telnet logon, press <Ctrl+K> or <Ctrl+]>.

If you do not specify a ***service_port***, the default Telnet port number of 23 is used.

Related command: **display tcp status**.

Example

To log in to the Ethernet switch Switch32 at IP address 10.1.1.1 from the current Switch (Switch01), enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]user-interface vty 0 4
[4500-ui-vty0-4]authentication-mode none
<Switch01>telnet 10.1.1.1
Trying 10.1.1.1.....
Press CTRL+K to abort
Connected to 10.1.1.1...
*******************************************************
*          All rights reserved (1997-2004)            *
*      Without the owner's prior written consent,     *
*no decompiling or reverse-engineering shall be allowed.*
*******************************************************
```

user-interface

Syntax

user-interface [*type*] *first_number* [*last_number*]

View

System view

Parameter

type: Enter the user interface type, which can be aux or vty.

first_number: Specifies the number of the first user interface to be configured.

last_number: Specifies the number of the last user interface to be configured.

Description

Using **user-interface** command, you can enter single user interface view or multiple user interface views to configure the corresponding user interfaces.

Example

To configure the user interfaces with index numbers 0 to 9, enter the following:

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]user-interface 0 9
[SW4500-ui0-9]
```

This example command selects two AUX (Console) port user interfaces and two VTY user interfaces (VTY 0, VTY 1). You can now assign access levels to these interfaces using the user privilege level command.

user privilege level

Syntax

user privilege level *level*

undo user privilege level

View

User interface view

Parameter

level: Enter the level of command that a user can access, in the range 0 to 3.

Description

Use the **user privilege level *level*** command to configure the command level that a user can access from the specified user interface. The user can use all the available commands at this command level. Use the **undo user privilege level** command to restore the default command level. By default, a user can access all commands at Level 3 after logging in through the AUX user interface, and all commands at Level 0 after logging in through a VTY user interface.

Example

To configure a user to access command level 0 after logging in from the VTY 0 user interface, enter the following:

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]user privilege level 0
```

When the user Telnets from the VTY 0 user interface to the switch, the terminal displays commands at level 0, as shown below:

```
<SW4500>?
User view commands:
   debugging       Debugging functions
   language-mode   Specify the language environment
   ping            Ping function
   quit            Exit from current command view
   super           Privilege current user a specified priority level
   telnet          Establish one TELNET connection
   tracert         Trace route function
   undo            Negate a command or set its default
```

2 USING PORT COMMANDS

This chapter describes how to use the following commands:

Ethernet Port Configuration Commands

Ethernet Port Link Aggregation Commands

- debugging link-aggregation event
- debugging lacp packet
- debugging lacp state
- display link-aggregation summary
- display link-aggregation verbose
- display link-aggregation interface
- display lacp system-id
- lacp enable
- lacp port-priority
- lacp system-priority
- link-aggregation group agg-id description
- link-aggregation group agg-id mode
- port link-aggregation group
- reset lacp statistics

Ethernet Port Configuration Commands

This section describes the commands you can use to configure and manage the ports on your Switch 4500.

copy configuration

Syntax

copy configuration source { *interface-type interface_number* | *interface_name* | aggregation-group *agg-id* } destination { *interface_list* [aggregation-group *agg-id*] | aggregation-group *agg-id* }

View

System View

Parameter

interface_type: Source port type.

interface_num: Source port number.

interface_name: Source port name, in the format of interface_name = interface_type interface_num. For more information, see the parameter item for the interface command.

interface_list: Destination port list, ***interface_list1*** = { ***interface_type interface_num*** | ***interface_name*** } [to { ***interface_type interface_num*** | ***interface_name*** }] &<1-10>. &<1-10> indicates that the former parameter can be input 10 times repeatedly at most.

agg-id: Source or destination aggregation group ID. If it is a source aggregation group, the port with minimum port number is the source port; if it is a destination aggregation group, the configurations of all its member ports change to be consistent with that of the source.

Description

Use the **copy configuration** command to copy the configuration of a specific port to other ports, to ensure consistent configuration.

Example

Copy the configuration of aggregation group 1 to aggregation group 2.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]copy configuration source ethernet 1/0/1 destination ethernet
1/0/2
Copying VLAN configuration...
Copying LACP configuration...
Copying QOS configuration...
Copying STP configuration...
Copying speed/duplex configuration...
[4500]
```

broadcast-suppression

Syntax

broadcast-suppression { ratio | pps *pps* }

undo broadcast-suppression

View

Ethernet Port View

Parameter

ratio: Specifies the bandwidth ratio of broadcast traffic allowed on an Ethernet port. The ratio value ranges from 1 to 100. The incremental step is 1. By default, the ratio is 100 meaning all broadcast traffic is accepted. The smaller the ratio is, the less bandwidth is allocated to broadcast traffic and therefore less broadcast traffic is accepted on the Ethernet port.

pps ***pps***: Specifies the maximum number of broadcast packets per second accepted on an Ethernet port. Ranges from 1 to 148810 pps.

Description

Use **broadcast-suppression** to configure the amount of broadcast traffic that will be accepted on a port. Once the broadcast traffic exceeds the value set by the user, the excess broadcast traffic will be discarded. This feature can be used to ensure network service and prevent broadcast storms.

Example

Enable a limit of 20% of the available bandwidth on a port to be allocated to broadcast traffic. Broadcast traffic exceeding 20% of the ports bandwidth will be discarded.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface ethernet 1/0/1
[4500-Ethernet1/0/1]broadcast-suppression 20
[4500-Ethernet1/0/1]
```

Specify the maximum packets per second of broadcast traffic on Ethernet1/0/1 to be 1000.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface ethernet 1/0/1
[4500-Ethernet1/0/1]broadcast-suppression pps 1000

[4500-Ethernet1/0/1]
```

description

Syntax

description ***text***

undo description

View

Ethernet Port View

Parameter

text: Enter a description of the Ethernet port. This can be a maximum of 80 characters.

Description

Use the **description** command to enter a description of an Ethernet port. Use the **undo description** command to cancel the description.

By default, an Ethernet port does not have a description.

Example

Set the description of port Ethernet1/0/1 to be lanswitch-interface.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface ethernet 1/0/1
[4500-Ethernet1/0/1]description lanswitch-interface
[4500-Ethernet1/0/1]
```

display interface

Syntax

display interface [***interface_type*** | ***interface_type interface_number*** **]**

View

All views

Parameter

interface_type: Enter the interface type. This can be either **Aux**, **Ethernet**, **GigabitEthernet** , **NULL, Vlan-interface**.

interface_number: Enter the interface number in the format unit-number/0/port-number.

The unit number is a number in the range 1 to 8.

The port number is a number in the range 1 to 28 or 1 to 52 depending on the number of ports you have on your unit.

You can use the ***interface_name*** *at this command. This consists of the* ***interface_type*** *and the* ***interface_number*** *combined as a single parameter. For example Ethernet1/0/1.*

Description

Use the **display interface** command to view the configuration information on the selected interface. Along with others, this interface could be a specific port's interface (for example, Ethernet1/0/1) or a specific VLAN interface (for example, vlan-interface 1).

Example

To display configuration information on Ethernet port 1/0/1, enter the following:

```
<4500>display interface Ethernet 1/0/1
```

The information displays in the following format:

```
Ethernet1/0/1 current state : UP
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is
00e0-fc00-0010
The Maximum Transmit Unit is 1500
Media type is twisted pair, loopback not set
Port hardware type is 100_BASE_TX
100Mbps-speed mode, full-duplex mode
Link speed type is autonegotiation, link duplex type is
autonegotiation
Flow-control is not enabled
The Maximum Frame Length is 1536
Broadcast MAX-ratio: 100%
Allow jumbo frame to pass
PVID: 1
Mdi type: auto
Port link-type: access
  Tagged   VLAN ID : none
  Untagged VLAN ID : 1
Last 300 seconds input:  0 packets/sec 0 bytes/sec
Last 300 seconds output:  0 packets/sec 0 bytes/sec
Input(total):  0 packets, 0 bytes
         - broadcasts, - multicasts
 Input(normal):  0 packets, 0 bytes
         0 broadcasts, 0 multicasts
 Input:  0 input errors, 0 runts, 0 giants,  0 throttles, 0 CRC
         0 frame,  - overruns, - aborts, - ignored, - parity errors
 Output(total): 0 packets, 0 bytes
         - broadcasts, - multicasts, - pauses
 Output(normal): 0 packets, 0 bytes
         0 broadcasts, 0 multicasts, 0 pauses
 Output: 0 output errors,  - underruns, - buffer failures
         - aborts, 0 deferred, 0 collisions, 0 late collisions
         - lost carrier, - no carrier
```

Table 6 Output Description of the Display Interface Command

Field	Description
Ethernet1/0/1 current state	Indicates the current state of the Ethernet port (up or down)
IP Sending frames' format	Displays the Ethernet frame format
Hardware address	Displays the port hardware address
Description	Displays the port description
The Maximum Transmit Unit	Indicates the maximum transmit unit
Media type	Indicates the type of media
loopback not set	Displays the port loopback test state
Port hardware type	Displays the port hardware type
100 Mbps-speed mode, full-duplex mode, link speed type is autonegotiation, link duplex type is autonegotiation	Indicates that the duplex mode and the rate have been auto-negotiated with the connected device, and have been set to 100 Mbps full-duplex.
Flow control is not enabled	Port flow control state
The Maximum Frame Length	Indicates the maximum length of the Ethernet frames that can pass through the port
Broadcast MAX ratio	Port broadcast storm suppression ratio

Table 6 Output Description of the Display Interface Command

Allow jumbo frame to pass	Indicates that jumbo frame are allowed to pass through the port
PVID	Indicates the port default VLAN ID.
Mdi type	Indicates the cable type
Port link-type	Indicates the port link type
Tagged VLAN ID	Indicates the VLANs with packets tagged
Untagged VLAN ID	Indicates the VLANs with packets untagged
Last 300 minutes input rate: 0 packets/sec, 0 bytes/sec Last 300 minutes output rate: 0 packets/sec, 0 bytes/sec	Displays the input/output rate and the number of packets that were passed on this port in the last 300 seconds
Input(total): 0 packets, 0 bytes - broadcasts, - multicasts Input(normal): 0 packets, 0 bytes 0 broadcasts, 0 multicasts Input: 0 input errors, 0 runts, 0 giants, 0 throttles, 0 CRC 0 frame, - overruns, - aborts, - ignored, - parity errors Output(total): 0 packets, 0 bytes - broadcasts, - multicasts, - pauses Output(normal): 0 packets, 0 bytes 0 broadcasts, 0 multicasts, 0 pauses Output: 0 output errors, - underruns, - buffer failures - aborts, 0 deferred, 0 collisions, 0 late collisions - lost carrier, - no carrier	The statistics information of input/output packets and errors on this port. A "-" indicates that the item isn't supported by the switch.

display loopback-detection

Syntax

display loopback-detection

View

All views

Parameter

None

Description

Use the **display loopback-detection** command to view whether the port loopback detection has been enabled. If it has been enabled, then the time interval of the detection and the current port loopback information will also be displayed.

Example

To display if the port loopback detection is enabled, enter the following:

```
<4500>display loopback-detection
```

The details display in the following format:

```
Port Ethernet1/0/1 loopback-detection is running
system Loopback-detection is running
Detection interval time is 30 seconds
There is no port existing loopback link
```

Table 7 Output Description of the Display Loopback-detection Command

Field	Description
Port Ethernet1/0/1 loopback-detection is running	
System Loopback-detection is running	System Loopback-detection is enabled
Detection interval time is 30 seconds	The detection interval is 30 seconds
There is no port existing loopback link	No port is in the loopback state

display port

Syntax

display port { hybrid | trunk }

View

All views

Parameter

hybrid: Enter to display the hybrid ports.

trunk: Enter to display the trunked ports.

Description

Use the **display port hybrid** command to view the ports whose link type is hybrid. Use the **display port trunk** command to view the ports whose link type is trunk.

Example

To display the currently configured hybrid ports, enter the following:

```
<4500>display port hybrid
```

The details display in the following format:

```
The following hybrid ports exist:
  Ethernet1/0/1          Ethernet1/0/2
```

This example indicates that the current configuration has two hybrid ports, Ethernet1/0/1 and Ethernet1/0/2.

display unit

Syntax

display unit *unit-id* interface

View

Any view

Parameter

unit-id: Specifies Unit ID, ranging from 1 to 8.

Description

Using **display unit *unit-id* interface** command, you can view all port interfaces for the specified unit.

Example

Display the port information for all ports on Unit 1.

```
<4500>display unit 1 interface
Aux1/0/0 current state :DOWN
Line protocol current state :DOWN
Internet protocol processing : disabled
Description :  Aux1/0/0 Interface
The Maximum Transmit Unit is 1500
Data drive mode: interactive
    5 minutes input rate 0.0 bytes/sec, 0.0 packets/sec
    5 minutes output rate 0.0 bytes/sec, 0.0 packets/sec
    0 packets input,  1000 bytes
    0 packets output,  27317 bytes
    error: Parity 0, Frame 0, Overrun 0, FIFO 0
DCD=UP  DTR=UP  DSR=UP  RTS=UP  CTS=UP
Ethernet1/0/1 current state : DOWN
 IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is
00e0-fc00-3900
(Omitted)
```

duplex

Syntax

duplex { auto | full | half }

undo duplex

View

Ethernet Port View

Parameters

auto: Enter to set the port to auto-negotiation.

full: Enter to set the port to full-duplex.

half: Enter to set the port to half-duplex.

Description

Use the **duplex** command to configure the duplex mode of an Ethernet port to auto-negotiation, full duplex or half-duplex. Use the **undo duplex** command to restore the duplex mode of a port to the default mode (auto-negotiation).

Related command: **speed**.

Example

To configure the Ethernet port "Ethernet1/0/1" to auto-negotiation, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface ethernet 1/0/1
```

```
[4500-Ethernet1/0/1]duplex auto
```

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 an Ethernet port. This avoids discarding data packets due to congestion. Use the **undo flow-control** command to disable flow control.

By default, flow control is disabled.

Example

To enable flow control on port "Ethernet1/0/1", enter the following.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface ethernet 1/0/1
[4500-Ethernet1/0/1]flow-control
[4500-Ethernet1/0/1]
```

interface

Syntax

interface ***interface_type interface_num*** | ***interface_name***

View

System View

Parameter

interface_type: Enter the interface type. This can be either **Aux**, **Ethernet**, **GigabitEthernet** , **NULL, Vlan-interface**.

interface_number: Enter the interface number in the format unit-number/0/port-number.

The unit number is a number in the range 1 to 8.

The port number is a number in the range 1 to 28 or 1 to 52 depending on the number of ports you have on your unit.

You can use the ***interface_name*** *at this command. This consists of the* ***interface_type*** *and the* ***interface_number*** *combined as a single parameter. For example Ethernet1/0/1.*

Description

Use the command **interface *interface_type interface_number*** to enter the interface of the specified port.

If you want to configure the parameters of an Ethernet port, you must first use this command to enter the Ethernet port view.

Example

To enter the interface for port "Ethernet1/0/1", enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface ethernet1/0/1
[4500-ethernet1/0/1]
```

loopback

Syntax

loopback { external | **internal }**

View

Ethernet Port View

Parameter

external: External loop test.

internal: Internal loop test.

Description

Use the **loopback** command to configure the Ethernet port to perform the loopback test to check if the Ethernet port works normally. The loop test will finish automatically after being performed for a while.

By default, the Ethernet port will not perform the loopback test.

Example

To perform the internal loop test for Ethernet1/0/1, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface ethernet 1/0/1
[4500-Ethernet1/0/1]loopback internal
#Apr  2 02:46:02:29 2000 4500 L2INF/2/PORT LINK STATUS CHANGE:- 1 -
 Trap 1.3.6.1.6.3.1.1.5.4: portIndex is 4227626, ifAdminStatus is 1,
ifOperStatus is 1

%Apr  2 02:46:02:225 2000 4500 L2INF/5/PORT LINK STATUS CHANGE:- 1 -
Ethernet1/0/1: is UP

%Apr  2 02:46:02:342 2000 4500 STP/2/SPEED:- 1 -Ethernet1/0/1's
speed changed
!
#Apr  2 02:46:02:521 2000 4500 L2INF/2/PORT LINK STATUS CHANGE:- 1
-Trap 1.3.6.1.6.3.1.1.5.3: portIndex is 4227626, ifAdminStatus is 1,
ifOperStatus is 2
```

```
Loop internal succeeded.
[4500-Ethernet1/0/1]
[4500-Ethernet1/0/1]loopback internal
```

loopback-detection control enable

Syntax

loopback-detection control enable

undo loopback-detection control enable

View

Ethernet Port View

Parameter

None

Description

Use the **loopback-detection control enable** command to enable loopback detection control function on a Trunk port or Hybrid port. Use the **undo loopback-detection control enable** command to disable loopback detection control function on a Trunk port or Hybrid port.

This command controls the operating status of the port, when the loopback detection function is enabled and loopback is detected on a Trunk or Hybrid port. When this function is enabled and loopback is detected on a Trunk or Hybrid port, the system begins to control the operating status of the port. When this function is disabled and loopback is found, the system just reports a Trap message but has no control over the operating status of the Trunk or Hybrid port.

By default, the loopback detection control function on Trunk or Hybrid ports is disabled.

This command has no effect on Access ports.

Example

Enable port loopback detection control.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface ethernet 1/0/1
[4500-Ethernet1/0/1]port link-type trunk
[4500-Ethernet1/0/1]loopback-detection control enable
[4500-Ethernet1/0/1]
```

loopback-detection enable

Syntax

loopback-detection enable

undo loopback-detection enable

View

Ethernet Port View

Parameter

None

Description

Use the `loopback-detection enable` command to enable port loopback detection. If there is a loopback port found, the switch will put it under control. Use the **`undo loopback-detection enable`** command to disable port loopback detection.

Loopback detection of a specified port only functions after port loopback detection is enabled in the System or Ethernet port view. By default, port loopback detection is disabled.

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

Example

To enable port loopback detection, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]loopback-detection enable
[4500]interface ethernet 1/0/1
[4500-Ethernet1/0/1]loopback-detection enable
[4500-Ethernet1/0/1]
```

loopback-detection interval-time

Syntax

`loopback-detection interval-time` ***`time`***

`undo loopback-detection interval-time`

View

System View

Parameter

`time:` Specifies the interval of monitoring external loopback conditions of the port. It ranges from 5 to 300, measured in seconds.

By default, the interval is 30 seconds.

Description

Use the **`loopback-detection interval-time`** command to configure the detection interval for the external loopback condition of each port. Use the **`undo loopback-detection interval-time`** command to restore the default interval.

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

Example

To configure the detection interval for the external loopback condition of each port to 10 seconds, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]loopback-detection interval-time 10
```

```
[4500]
```

loopback-detection per-vlan enable

Syntax

loopback-detection per-vlan enable

undo loopback-detection per-vlan enable

View

Ethernet Port View

Parameter

None

Description

Use the **loopback-detection per-vlan enable** command to configure the system to perform loopback detection on all VLANs on Trunk and Hybrid ports. Use the **undo loopback-detection per-vlan enable** command to configure the system to only perform loopback detection on the default VLANs on the port.

By default, the system performs loopback detection to the default VLAN on Trunk and Hybrid ports.

Example

Configure the detection interval for the external loopback condition of each port to 10 seconds.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface ethernet 1/0/1
[4500-Ethernet1/0/1]port link-type trunk
[4500-Ethernet1/0/1]loopback-detection per-vlan enable
[4500-Ethernet1/0/1]
```

mdi

Syntax

mdi { across | auto | normal }

undo mdi

View

Ethernet Port View

Parameter

across: Enter to configure the network cable type to cross-over cable. Not available on the Switch 4500.

auto: Enter to configure the use of either straight-through cable or cross-over cable.

normal: Enter to configure the network cable type to straight-through cable. Not available on the Switch 4500.

Description

- Use the **mdi** command to configure the network cable type for an Ethernet port.
- Use the **undo mdi** command to restore the default type. By default, the network cable type is recognized automatically (the **mdi auto** command).

Note that this command only has effect on 10/100BASE-T and 10/100/1000BASE-T ports. The Switch 4500 only supports **auto** (auto-sensing). If you enter another type, an error message displays.

Example

To configure the network cable type of port "Ethernet1/0/1" as cross-over cable, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface ethernet 1/0/1
[4500-Ethernet1/0/1]mdi across
[4500-Ethernet1/0/1]
```

multicast-suppression

Syntax

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

undo multicast-suppression

View

Ethernet Port View

Parameter

ratio: Specifies the bandwidth ratio of multicast traffic allowed on an Ethernet port. The ratio value ranges from 1 to 100. The incremental step is 1. By default, the ratio is 100 meaning all multicast traffic is accepted. The smaller the ratio is, the less bandwidth is allocated to multicast traffic and therefore less broadcast traffic is accepted on the Ethernet port.

pps ***pps***: Specifies the maximum number of multicast packets per second accepted on an Ethernet port. Ranges from 1 to 148810 pps.

Description

Use **multicast-suppression** to configure the amount of multicast traffic that will be accepted on a port. Once the multicast traffic exceeds the value set by the user, the excess multicast traffic will be discarded. This feature can be used to ensure network service and prevent multicast storms.

Example

Enable a limit of 20% of the available bandwidth on a port to be allocated to multicast traffic. Multicast traffic exceeding 20% of the ports bandwidth will be discarded.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface ethernet 1/0/1
```

```
[4500-Ethernet1/0/1]multicast-suppression 20
[4500-Ethernet1/0/1]
```

Specify the maximum packets per second of the multicast traffic on an Ethernet1/0/1 as 1000 Mpps.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface ethernet 1/0/1
[4500-Ethernet1/0/1]multicast-suppression pps 1000
[4500-Ethernet1/0/1]
```

port access vlan

Syntax

port access vlan *vlan_id*

undo port access vlan

View

Ethernet Port View

Parameter

vlan_id: Enter a VLAN ID in the range 2 to 4094, as defined in IEEE 802.1Q.

Description

- Use the **port access vlan** command to assign the access port to a specified VLAN.
- Use the **undo port access vlan** command to remove the access port from the VLAN.

Example

To assign Ethernet port 1/0/1 to VLAN3, enter the following.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]vlan 3
[4500-vlan3]quit
[4500]interface ethernet 1/0/1
[4500-Ethernet1/0/1]port access vlan 3
[4500-Ethernet1/0/1]
```

port hybrid pvid vlan

Syntax

port hybrid pvid vlan *vlan_id*

undo port hybrid pvid

View

Ethernet Port View

Parameter

vlan_id: Enter a VLAN ID in the range 2 to 4094, as defined in IEEE 802.1Q. The default is 1.

Description

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

Hybrid port can be configured together with the isolate-user-vlan. But if the default VLAN has set mapping in the isolate-user-vlan, the default VLAN ID cannot be modified. If you want to modify it, cancel the mapping first.

The default VLAN ID of local hybrid port must be consistent with that of the peer one, otherwise, the packets cannot be properly transmitted.

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

Example

To configure the default VLAN of the hybrid port Ethernet1/0/1 to VLAN100, enter the following.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface ethernet 1/0/1
[4500-Ethernet1/0/1]port link-type hybrid
[4500-Ethernet1/0/1]port hybrid pvid vlan 100
[4500-Ethernet1/0/1]
```

port hybrid vlan

Syntax

port hybrid vlan ***vlan_id_list*** **{ tagged** | **untagged }**

undo port hybrid vlan ***vlan_id_list***

View

Ethernet Port View

Parameter

vlan_id_list: Enter a VLAN ID, or more than one VLAN ID, in the range 2 to 4094. The hybrid port will be added to the specified VLANs. This can be a single VLAN, a series of individual VLANs separated by a space, or the first VLAN in a range of VLANs (***vlan_id*** **to** ***last_vlan_id***).

You can enter up to ten **vlan_id** *parameters in one* **port hybrid vlan** *command.*

tagged: Enter to tag the port for the specified VLAN.

untagged: Enter to leave the port untagged for the specified VLAN.

Description

Use the **port hybrid vlan** command to add the port to the specified VLAN(s). The port needs to have been made a hybrid port before you can do this. See the related command below. Use the **undo port hybrid vlan** command to remove the port from the specified VLAN(s).

A hybrid port can belong to multiple VLANs. A port can only be added to a VLAN if the VLAN has already been created. See the **vlan vlan-vid** command.

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

Example

To add the port Ethernet1/0/1 to VLAN 2, VLAN 4 and all VLANs in the range 50 to 100 as a tagged port, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface ethernet 1/0/1
[4500-Ethernet1/0/1]port link-type hybrid
[4500-Ethernet1/0/1]quit
[4500]vlan 2
[4500-vlan2]quit
[4500]interface e1/0/1
[4500-Ethernet1/0/1]port hybrid vlan 2 4 50 to 100 tagged
[4500-Ethernet1/0/1]
```

port link-type

Syntax

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

undo port link-type

View

Ethernet Port View

Parameter

access: Enter to configure the port as an access port.

hybrid: Enter to configure the port as a hybrid port

trunk: Enter to configure the port as a trunk port.

xrn-fabric: Enter to configure the port as a Fabric port.

Description

Use the **port link-type** command to configure the link type of the Ethernet port. Use the **undo port link-type** command to restore the port as default status. By default, a port is an access port.

A port on a Switch can be configured as an access port, a hybrid port, a trunk port or a fabric port. However, to reconfigure between hybrid and trunk link types, you must first restore the default, or access, link type.

Only the Gigabit combo ports can be used to interconnect the Switch units to form a stack.

Example

To configure the Ethernet port Ethernet1/0/1 as a trunk port, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
```

```
[4500]interface ethernet 1/0/1
[4500-Ethernet1/0/1]port link-type trunk
[4500-Ethernet1/0/1]
```

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

Parameter

vlan_id: Enter a VLAN ID, or more than one VLAN ID, in the range 2 to 4094. The trunk port will be added to the specified VLANs. This can be a single VLAN, a series of individual VLANs separated by a space, or the first VLAN in a range of VLANs. If this is the first VLAN in a range use the ***last_vlan_id*** parameter to indicate the last VLAN in the range (***vlan_id* to *last_vlan_id***).

You can enter up to ten **vlan_id** *parameters at one* **port trunk permit vlan** *command.*

all: Enter to add the trunk port to all VLANs.

Description

Use the **port trunk permit vlan** command to add a trunk port to one VLAN, a selection of VLANs or all VLANs. Use the **undo port trunk permit vlan** command to remove a trunk port from one VLAN, a selection of VLANs or all VLANs.

A trunk port can belong to multiple VLANs. If the **port trunk permit vlan** command is used many times, then the VLAN enabled to pass on trunk port is the set of these ***vlan_id_list***.

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

Example

To add the trunk port Ethernet1/0/1 to VLAN 2, VLAN 4 and all VLANs in the range 50-100, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface ethernet 1/0/1
[4500-Ethernet1/0/1]port link-type trunk
[4500-Ethernet1/0/1]port trunk permit vlan 2 4 50 to 100
Please wait... Done.
[4500-Ethernet1/0/1]
```

port trunk pvid vlan

Syntax

port trunk pvid vlan *vlan_id*

undo port trunk pvid

View

Ethernet Port View

Parameter

vlan_id: Enter a VLAN ID in the range 2 to 4094, as defined in IEEE802.1Q. This is the VLAN that you want to be the default VLAN for a trunk port.
The default is 1.

Description

Use the **port trunk pvid vlan** command to configure the default VLAN ID for a trunk port. Use the **undo port trunk pvid** command to restore the default VLAN ID for a trunk port.

The default VLAN ID of local trunk port should be consistent with that of the peer one, otherwise packets cannot be properly transmitted.

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

Example

To configure the trunk port Ethernet1/0/1 to the default VLAN of 100, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface ethernet 1/0/1
[4500-Ethernet1/0/1]port link-type trunk
[4500-Ethernet1/0/1]port trunk pvid vlan 100
[4500-Ethernet1/0/1]
```

reset counters interface

Syntax

reset counters interface [***interface_type*** | ***interface_type interface_num*** | ***interface_name*****]**

View

User view

Parameter

interface_type: Specifies the port type.

interface_num: Specifies the port number.

interface_name: Specifies the port name in the ***interface_name= interface_type interface_num*** format.

For parameter description, refer to the **interface** command.

Description

Use the **reset counters interface** command to reset the statistical information on the port and count the related information again on the port for the user.

If you do not enter a port type, or port type and port number, information is cleared from all ports on the Switch. If only the port type is specified, all the information on ports of this type will be cleared. If both port type and port

number are specified, the information on the specified port will be cleared. After 802.1x is enabled, the port information cannot be reset.

Example

To reset statistical information on Ethernet1/0/1, enter the following:

```
<4500>reset counters interface ethernet1/0/1
<4500>
```

shutdown

Syntax

shutdown

undo shutdown

View

Ethernet Port View

Parameter

None

Description

Use the **shutdown** command to disable an Ethernet port. Use the **undo shutdown** command to enable an Ethernet port.

By default, the Ethernet port is enabled.

Example

To disable and then enable Ethernet1/0/1, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface ethernet 1/0/1
[4500-Ethernet1/0/1]shutdown
[4500-Ethernet1/0/1]undo shutdown
```

speed

Syntax

For a 100 Mbps Ethernet port, the parameters for this command are as follows:

speed { 10 | 100 | auto }

For a 1000 Mbps Ethernet port, the parameters for this command are as follows:

speed { 10 | 100 | 1000 | auto }

The undo form of this command is:

undo speed

View

Ethernet Port View

Parameter

10: Enter to set the port speed to 10 Mbps.

100: Enter to set the port speed to 100 Mbps.

1000: Enter to set the port speed to 1000 Mbps. (Only available on Gigabit ports).

auto: Enter to set the port speed to auto-negotiation.

Description

Use the **speed** command to configure the port speed. Use the **undo speed** command to restore the default speed. By default, the speed is **auto**.

Related command: **duplex**.

Example

To configure the port speed of port Ethernet1/0/1 to 10 Mbps, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface ethernet 1/0/1
[4500-Ethernet1/0/1]speed 10
[4500-Ethernet1/0/1]
```

unicast-suppression

Syntax

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

undo unicast-suppression

View

Ethernet Port View

Parameter

ratio: Specifies the bandwidth ratio of unicast traffic allowed on an Ethernet port. The ratio value ranges from 1 to 100. The incremental step is 1. By default, the ratio is 100 meaning all unicast traffic is accepted. The smaller the ratio is, the less bandwidth is allocated to unicast traffic and therefore less broadcast traffic is accepted on the Ethernet port.

pps *pps*: Specifies the maximum number of unicast packets per second accepted on an Ethernet port. Ranges from 1 to 148810 pps.

Description

Use **unicast-suppression** to configure the amount of unicast traffic that will be accepted on a port. Once the multicast traffic exceeds the value set by the user, the excess unicast traffic will be discarded. This feature can be used to ensure network service and prevent unicast storms.

Example

Enable a limit of 20% of the available bandwidth on a port to be allocated to unicast traffic. Unicast traffic exceeding 20% of the ports bandwidth will be discarded.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface ethernet 1/0/1
```

```
[4500-Ethernet1/0/1]unicast-suppression 20
[4500-Ethernet1/0/1]
```

Specify the maximum packets per second of the unicast traffic on an Ethernet1/0/1 as 1000 Mpps.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface ethernet 1/0/1
[4500-Ethernet1/0/1]unicast-suppression pps 1000
[4500-Ethernet1/0/1]
```

Ethernet Port Link Aggregation Commands

This section describes the commands you can use to configure Ethernet Port LInk Aggregation on the Switch.

debugging link-aggregation error

Syntax

debugging link-aggregation error

undo debugging link-aggregation error

View

User View

Parameter

None

Description

Use the **debugging link-aggregation error** command to enable link aggregation error debugging. Use the **undo debugging link-aggregation error** command to disable link aggregation error debugging.

Example

To enable link aggregation error debugging, enter the following:

```
<4500>debugging link-aggregation error
```

debugging link-aggregation event

Syntax

debugging link-aggregation event

undo debugging link-aggregation event

View

User View

Parameter

None

Description

Use the **debugging link-aggregation** event command to enable link aggregation events debugging. Use the **undo debugging link-aggregation event** command to disable link aggregation events debugging.

Example

To enable link aggregation events debugging, enter the following:

```
<4500>debugging link-aggregation event
```

debugging lacp packet

Syntax

debugging lacp packet [interface { *interface_type interface_number* | *interface_name* } [to { *interface_type interface_num* | *interface_name* }]]

undo debugging lacp packet [interface { *interface_type interface_number* | *interface_name* } [to { *interface_type interface_num* | *interface_name* }]]

View

User View

Parameter

interface { ***interface_type interface_ num*** | ***interface_name*** } [**to** { ***interface_type interface_ num*** | ***interface_name*** }]: Specifies ports. You can specify multiple sequential ports with the **to** parameter, instead of specifying only one port.

interface_name: Specifies port name, in the format of ***interface_name = interface_type interface_num.***

interface_type: Specifies port type and ***interface_num*** port number.

For more information, see the parameter item for the **interface** command.

Description

Use the **debugging lacp packet** command to enable LACP packets debugging at a designated port or ports. Use the **undo debugging lacp packet** command to disable LACP packets debugging at a designated port or ports.

Example

To enable LACP packets debugging at Ethernet1/0/1, enter the following:

```
<4500>debugging lacp packet interface ethernet1/0/1
```

debugging lacp state

Syntax

debugging lacp state [**interface** { ***interface_type interface_number*** | ***interface_name*** } [**to** { ***interface_type interface_num*** | ***interface_name*** }]] { { **actor-churn** | **mux** | **partner-churn** | **ptx** | **rx** }* | **all** }

undo debugging lacp state [**interface** { ***interface_type interface_number*** | ***interface_name*** } [**to** { ***interface_type interface_num*** | ***interface_name*** }]] { { **actor-churn** | **mux** | **partner-churn** | **ptx** | **rx** }* | **all** }

View

User View

Parameter

interface { ***interface_type interface_num*** | ***interface_name*** } [**to** { ***interface_type interface_num*** | ***interface_name*** }]: Specifies ports. You can specify multiple sequential ports with the **to** parameter, instead of specifying only one port.

interface_name: Specifies port name, in the format of ***interface_name = interface_type interface_num.***

interface_type: Specifies port type and ***interface_num*** port number.

For more information, see the parameter item for the **interface** command.

actor-churn: Debugging actor-churn state machine.

mux: Debugging MUX state machine.

partner-churn: Debugging partner-churn state machine.

ptx: Debugging PTX state machine.

rx: Debugging RX state machine.

all: Debugging all state machines.

Description

Use the **debugging lacp state** command to enable LACP state machines debugging on a designated port or ports. Use the **undo debugging lacp state** command to disable LACP state machines debugging on a designated port or ports.

Example

To enable all LACP state machines debugging.

```
<4500>debugging lacp state all
```

display link-aggregation summary

Syntax

display link-aggregation summary

View

Any view

Parameter

None

Description

Use the **display link-aggregation summary** command to view summary information of all aggregation groups, including actor system ID, aggregation group ID, aggregate group type, partner system ID, number of selected ports, number of standby ports, load sharing type and master port number.

Example

To display summary information of all aggregation information, enter the following:

```
<4500>display link-aggregation summary
Aggregation Group Type: D -- Dynamic, S -- Static, M -- Manual
Loadsharing Type: Shar – Loadsharing, NonS – Non-Loadsharing
Actor ID: 0x8000, 00e0-fcff-ff04
```

```
AL    AL    Partner ID           Select  Standby Share   Master
ID    Type                       Ports   Ports   Type    Port
-------------------------------------------------------------------
1     D     0x8000,00e0-fcff-ff01 1       0       NonS  Ethernet4/0/1
10    M     none                  1       0       NonS  Ethernet4/0/2
20    S     0x8000,00e0-fcff-ff01 1       0       NonS  Ethernet4/0/3
```

display link-aggregation verbose

Syntax

display link-aggregation verbose [*agg_id*]

View

Any view

Parameter

agg_id: Aggregation group ID, which must be a valid existing ID, in the range of 1 to 416.

Description

Use the **display link-aggregation verbose** command to view detailed information of a link aggregation, including aggregation ID, the type of aggregation, load-sharing type, detailed local information (member ports, port status, port priority, LACP state flag and operation key), and detailed remote information (indexes of remote ports, port priority, LACP state flag, operation key and system ID.)

Note that unlike a dynamic aggregation, a manual aggregation has no protocol to get the remote peer information of the partner. Therefore, every item for the remote peer is 0. This does not indicate the actual state of the remote peer.

Example

To display detailed information of aggregation group 1, enter the following:

```
<4500>display link-aggregation verbose 1
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing

Aggregation ID: 1,  AggregationType: Manual,   Loadsharing Type: NonS
Aggregation Description:
System ID: 0x8000, 000f-cbb7-2e00
Port Status: S -- Selected,  U -- Unselected
Local:
    Port                    Status  Priority Flag Oper-Key
-------------------------------------------------------------------
    Ethernet1/0/2           U       32768    0x00 1
    Ethernet1/0/3           U       32768    0x00 1
    Ethernet1/0/4           S       32768    0x00 1

Remote:
    Actor          Partner Priority Flag Oper-Key SystemID
-------------------------------------------------------------------
    Ethernet1/0/2    0       0       0x00 0 0x0,0000-0000-0000
    Ethernet1/0/3    0       0       0x00  0 0x0,0000-0000-0000
    Ethernet1/0/4    0       0       0x00 0 0x0,0000-0000-0000
<4500>
```

display link-aggregation interface

Syntax

display link-aggregation interface { ***interface_type interface_number*** | ***interface_name*** } [**to** { ***interface_type interface-num*** | ***interface_name*** }]

View

Any view

Parameter

interface { ***interface_type interface_ num*** | ***interface_name*** } [**to** { ***interface_type interface_ num*** | ***interface_name*** }]: Specifies ports. You can specify multiple sequential ports with the **to** parameter, instead of specifying only one port.

interface_name: Specifies port name, in the format of ***interface_name = interface_type interface_num.***

interface_type: Specifies port type and ***interface_num*** port number.

For more information, see the parameter item for the **interface** command.

Description

Use the **display link-aggregation interface** command to view detailed link aggregation information at a designated port, including aggregation group ID for the port, port priority, operation key, LACP state flag, partner information (system ID, port number, port priority, operation key, LACP state flag, LACP packet statistics).

Note that unlike a dynamic aggregation, a manual aggregation has no protocol to get the remote peer information of the partner. Therefore, every item for the remote peer is 0. This does not indicate the actual state of the remote peer.

Example

To display detailed link aggregation information of a link aggregation member port, enter the following:

```
<4500>display link-aggregation interface ethernet4/0/1
```

If the aggregation has been created manually, the display will be similar to the following:

```
Ethernet4/0/1:
   Attached AggID: 1
   Local:
     Port-Priority: 32768, Oper key: 1, Flag: 0x00
   Remote:
     System ID: 0x0, 0000-0000-0000
     Port Number: 0, Port-Priority: 0, Oper-key: 0, Flag: 0x00
```

If the aggregation is static or dynamic, the display will be similar to the following:

```
<4500>display link-aggregation interface ethernet4/0/1
Ethernet4/0/1:
   Attached AggID: 20
```

```
Local:
  Port-Priority: 32768, Oper key: 2, Flag: 0x3d
Remote:
  System ID: 0x8000, 000e-84a6-fb00
  Port Number: 2, Port-Priority: 32768 , Oper-key: 10, Flag: 0x3d
Received LACP Packets: 8 packet(s), Illegal: 0 packet(s)
Sent LACP Packets: 9 packet(s)
```

Related command: **display link-aggregation verbose**.

display lacp system-id

Syntax

display lacp system-id

View

Any view

Parameter

None

Description

Use the **display lacp system-id** command to view actor system ID, including system priority and system MAC address.

Related command: **link-aggregation**.

Example

To display the local system ID.

```
<4500>display lacp system-id
Actor System ID: 0x8000, 00e0-fc00-0100
```

lacp enable

Syntax

lacp enable

undo lacp enable

View

Ethernet Port View

Parameter

None

Description

Use the **lacp enable** command to enable LACP.

Use the **undo lacp enable** command to disable LACP.

The Switch will select the lowest port number as the master port for the link aggregation. This applies to all types of link aggregation. If the aggregation spans a stack of units (only avaliable on the Switch 4500-EI) and the same ports are used, the unit number will be the tie-breaker. For example, 1/0/1 and 2/0/1 are in an aggregation. Port 1/0/1 will be the master port.

Example

To enable LACP at Ethernet1/0/1, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface ethernet 1/0/1
[4500-Ethernet1/0/1]lacp enable
[4500-Ethernet1/0/1]
```

lacp port-priority

Syntax

lacp port-priority ***port-priority-value***

undo lacp port-priority

View

Ethernet Port View

Parameter

port-priority-value: Port priority, ranging from 0 to 65535. By default, it is 32768.

Description

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

Related commands: **display link-aggregation verbose** and **display link-aggregation interface**.

Example

To set port priority as 64, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface ethernet 1/0/1
[4500-Ethernet1/0/1]lacp port-priority 64
[4500-Ethernet1/0/1]
```

lacp system-priority

Syntax

lacp system-priority ***system-priority-value***

undo lacp system-priority

View

System View

Parameter

system-priority-value: System priority, ranging from 0 to 65535. By default, it is 32768.

Description

Use the **lacp system-priority** command to configure system priority value.

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

Related command: **display lacp system-id**.

Example

To set system priority as 64, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]lacp system-priority 64
[4500]
```

link-aggregation group agg-id description

Syntax

link-aggregation group *agg_id* description *alname*

undo link-aggregation group agg-id description

View

System View

Parameter

agg_id: Aggregation group ID, in the range of 1 to 416.

alname: Aggregation group name, character string with 1 to 32 characters.

Description

Use the **link-aggregation group *agg_id* description** command to configure descriptor for an aggregation group. Use the **undo link-aggregation group agg-id description** command to delete aggregation group descriptor.

Related command: **display link-aggregation verbose**.

Example

To configure myal1 as the descriptor of aggregation group 22, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]link-aggregation group 22 mode manual
[4500]link-aggregation group 22 description myal1
[4500]
```

link-aggregation group agg-id mode

Syntax

link-aggregation group *agg_id* mode { manual | static }

undo link-aggregation group *agg_id*

View

System View

Parameter

agg_id: Aggregation group ID, in the range of 1 to 416.

manual: Manual aggregation group.

static: Static aggregation group.

Description

Use the **link-aggregation group *agg_id* mode** command to create a manual or static aggregation group. Use the **undo link-aggregation group** command to delete an aggregation group.

The Switch will select the lowest port number as the master port for the link aggregation. This applies to all types of link aggregation. If the aggregation spans a stack of units and the same ports are used, the unit number will be the tie-breaker. For example, 1/0/1 and 2/0/1 are in an aggregation. Port 1/0/1 will be the master port.

A manual or static aggregation group can have up to eight ports. You can use the **link-aggregation group *agg-id* mode** command to change an existing dynamic aggregation group into a manual or static one. If the port number in a group exceeds eight, this operation fails and the system prompts you about the configuration failure.

Related command: **display link-aggregation summary**.

Example

To create manual aggregation group 22, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]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

Parameter

agg_id: Aggregation group ID, in the range of 1 to 416.

Description

Use the **port link-aggregation group *agg_id*** command to add an Ethernet port into a manual or static aggregation group. Use the **undo port link-aggregation group** command, to delete an Ethernet port from a manual or static aggregation group.

Related command: **display link-aggregation verbose**.

Example

To add Ethernet1/0/1 into aggregation group 22, enter the following:

```
<4500>system-view
```

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

[4500]link-aggregation group 22 mode manual

[4500]interface ethernet 1/0/1

[4500-Ethernet1/0/1]port link-aggregation group 22

#Apr  2 03:29:48:954 2000 4500 LAGG/2/AggPortInactive:- 1 -Trap
1.3.6.1.4.1.2

011.5.25.25.2.2: TrapIndex 31465473 Aggregation Group 22: port
member Ethernet1/

0/1 becomes INACTIVE!

[4500-Ethernet1/0/1]
```

reset lacp statistics

Syntax

reset lacp statistics [**interface** { ***interface_type interface_number*** | ***interface_name*** } [**to** { ***interface_type interface_num*** | ***interface_name*** }]]

View

User View

Parameter

interface { ***interface_type interface_ num*** | ***interface_name*** } [**to** { ***interface_type interface_ num*** | ***interface_name*** }]: Specifies ports. You can specify multiple sequential ports with the **to** parameter, instead of specifying only one port.

interface_name: Specifies port name, in the format of ***interface_name = interface_type interface_num.***

interface_type: Specifies port type and ***interface_num*** port number.

For more information, see the parameter item for the **interface** command.

Description

Use the **reset lacp statistics** command to clear LACP statistics at a designated port. If no port is specified, then LACP statistics at all ports shall be cleared.

Related command: **display link-aggregation interface**.

Example

To clear LACP statistics at all Ethernet ports, enter the following:

```
<4500>reset lacp statistics
```

3 USING VLAN COMMANDS

This chapter describes how to use the following commands:

VLAN Configuration Commands

- description
- display interface VLAN-interface
- display vlan
- interface VLAN-interface_
- shutdown
- vlan

Voice VLAN Commands

- display voice vlan oui
- display voice vlan status
- voice vlan aging
- voice vlan enable
- voice vlan
- voice vlan mac_address
- voice vlan mode
- voice vlan security enable

VLAN Configuration Commands

This section describes the commands you can use to configure and manage the VLANs and VLAN interfaces on your system.

description

Syntax

description *string*

undo description

View

VLAN view

Parameter

string: Enter a description of the current VLAN, up to a maximum of 32 characters. For a description of a VLAN interface, the maximum is 80 characters.

Description

Use the description command to set a description for the current VLAN. Use the **undo description** command to cancel the description of current VLAN.

The default description character string of the current VLAN is `no description!`. The default description character string of the VLAN interface is the interface name, for example, `vlan-interface1`.

Related command: **display vlan**.

Example

To give VLAN1 the description "RESEARCH", enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]vlan 1
[4500-vlan1]description RESEARCH
[4500-vlan1]
```

display interface VLAN-interface

Syntax

display interface vlan-interface [*vlan_id*]

View

All views

Parameter

vlan_id: Enter the ID number of the VLAN interface, ranging from 1 to 4094.

Description

Use the **display interface vlan-interface** command to view the information about a specific VLAN interface, or all VLAN interfaces. The information displayed includes:

- Current status of the interface
- Current status of the line protocol

- VLAN interface description
- Maximum Transmit Unit (MTU)
- IP address and subnet mask
- Format of the IP frames
- MAC hardware address.

Use **display interface vlan-interface** to display information on all VLAN interfaces. Use **display interface vlan-interface *vlan_id*** to display information on a specific VLAN interface

Related command: **interface Vlan-interface**.

Example

To display information on VLAN interface 1, enter the following:

```
<4500>display interface vlan-interface 1
```

The information displays in the following format:

```
Vlan-interface1 current state :UP
Line protocol current state :UP
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is
00e0-fc00-3971
Internet Address is 161.71.61.206/24 Primary
Description :  Vlan-interface1 Interface
The Maximum Transmit Unit is 1500

<4500>
```

display vlan

Syntax

display vlan [*vlan_id* | all | static | dynamic]

View

All views

Parameter

vlan_id: Enter to display information on a specified VLAN.

all: Enter to display information on all VLANs.

static: Enter to display information on VLANs created statically by the system.

dynamic: Enter to display information on VLANs created dynamically by the system.

Description

Use the **display vlan** command to view related information about specific VLANs, specific types of VLAN or all VLANs. The information includes: VLAN type, whether the Route interface has been configured on the VLAN, the Broadcast Suppression max-ratio, the VLAN description, and a list of the tagged and untagged ports that belong to the VLAN. Use the command **display vlan** to display a summary of the VLAN IDs of all VLANs configured on the system. Use the

command **display vlan *vlan_id*** to display information on a specific VLAN. Use the command **display vlan all** to display information on all the VLANs. Use the command **display vlan dynamic** to display information on VLANs created dynamically by the system. Use the command **display vlan static** to display information of VLAN created statically by the system.

Related command: **vlan**.

Examples

To display information about VLAN 1:

```
<4500>display vlan 1
VLAN ID: 1

 VLAN Type: static
 Route Interface: configured
 IP Address: 161.71.61.206
 Subnet Mask: 255.255.255.0
 Description: VLAN 0001
 Tagged   Ports:
   GigabitEthernet1/0/52 GigabitEthernet2/0/27
 Untagged Ports:
   Ethernet1/0/1         Ethernet1/0/2         Ethernet1/0/3
   Ethernet1/0/4         Ethernet1/0/5         Ethernet1/0/6
   Ethernet1/0/7         Ethernet1/0/8         Ethernet1/0/9
   Ethernet1/0/10        Ethernet1/0/11        Ethernet1/0/12
   Ethernet1/0/13        Ethernet1/0/14        Ethernet1/0/15
   Ethernet1/0/16        Ethernet1/0/17        Ethernet1/0/18
   Ethernet1/0/19        Ethernet1/0/20        Ethernet1/0/21
   Ethernet1/0/22        Ethernet1/0/23        Ethernet1/0/24
   Ethernet1/0/25        Ethernet1/0/26        Ethernet1/0/27
   Ethernet1/0/28        Ethernet1/0/29        Ethernet1/0/30
   Ethernet1/0/31        Ethernet1/0/32        Ethernet1/0/33
   Ethernet1/0/34        Ethernet1/0/35        Ethernet1/0/36
   Ethernet1/0/37        Ethernet1/0/38        Ethernet1/0/39
   Ethernet1/0/40        Ethernet1/0/41        Ethernet1/0/42
   Ethernet1/0/43        Ethernet1/0/44        Ethernet1/0/45
   Ethernet1/0/46        Ethernet1/0/47        Ethernet1/0/48
   GigabitEthernet1/0/50 GigabitEthernet1/0/51 Ethernet2/0/1
   Ethernet2/0/2         Ethernet2/0/3         Ethernet2/0/4
   Ethernet2/0/5         Ethernet2/0/6         Ethernet2/0/7
   Ethernet2/0/8         Ethernet2/0/9         Ethernet2/0/10
   Ethernet2/0/11        Ethernet2/0/12        Ethernet2/0/13
   Ethernet2/0/14        Ethernet2/0/15        Ethernet2/0/16
   Ethernet2/0/17        Ethernet2/0/18        Ethernet2/0/19
   Ethernet2/0/20        Ethernet2/0/21        Ethernet2/0/22
   Ethernet2/0/23          Ethernet2/0/24 GigabitEthernet2/0/25
   GigabitEthernet2/0/26 GigabitEthernet2/0/28

<4500>
```

interface VLAN-interface

Syntax

interface vlan-interface *vlan_id*

undo interface vlan-interface *vlan_id*

View

System View

Parameter

vlan_id: Enter the ID of the VLAN interface you want to configure, in the range 1 to 4094. Note that VLAN1 is the default VLAN and cannot be deleted.

Description

Use the **interface vlan-interface** command to enter a VLAN interface view and use the related configuration commands. Use the **undo interface vlan-interface** command to exit the current VLAN interface.

Related command: **display interface vlan-interface**.

Example

To enter the interface view of VLAN1, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500] interface vlan-interface 1
[4500-Vlan-interface1]
```

port

Syntax

port ***interface_list***

undo port ***interface_list***

View

VLAN view

Parameter

interface_list: list of Ethernet ports to be added to or deleted from a certain VLAN, expressed as *interface_list*= {{ *interface_type interface_num* | *interface_name* } [**to** { *interface_type interface_num* | *interface_name* }] }**&<1-10>**.

interface_type is the interface type, *interface_num* is the interface number and *interface_name* is the interface name. For their meanings and value range, see the parameter of **Port** in this document. The interface number after keyword **to** must be larger than or equal to the port number before **to**.

&<1-10>: Represents the repeatable times of parameters, 1 is the minimal and 10 is the maximal.

Description

Using the **port** command, you can add one port or one group of ports to a VLAN. Using the **undo port** command, you can cancel one port or one group of ports from a VLAN.

You can add/delete trunk port and hybrid ports to/from a VLAN by **port** *and* **undo port** *commands in Ethernet Port View, but not in VLAN View.*

For the related command, see **display vlan**.

Example

Add Ethernet1/0/2 through Ethernet1/0/4 to VLAN 2.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]vlan 2
[4500-vlan2]port ethernet1/0/2 to ethernet1/0/4
```

shutdown

Syntax

shutdown

undo shutdown

View

VLAN Interface View

Parameter

None

Description

Use the **shutdown** command to disable the VLAN interface. Use the **undo shutdown** command to enable the VLAN interface.

By default, when all Ethernet ports are in DOWN status in VLAN interface, the VLAN interface is in DOWN status and is disabled. When there is one or more Ethernet ports in VLAN interface are in UP status, the VLAN interface is UP.

This command can be used to start the interface after the related parameters and protocols of VLAN interface are set. Or when the VLAN interface fails, the interface can be shut down first and then restarted, in this way, the interface may be restored to normal status. Shutting down or starting VLAN interface will not take any effect on any Ethernet port of this VLAN.

Example

Restart interface after shutting down the interface.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]vlan 2
[4500-vlan2]quit
[4500]interface vlan-interface 2
[4500-Vlan-interface2]shutdown
%Apr  2 00:06:15:277 2000 4500 L2INF/5/VLANIF LINK STATUS CHANGE:- 1
- Vlan-interface1: is DOWN

[4500-Vlan-interface2]undo shutdown

#Apr  2 00:05:27:793 2000 4500 L2INF/2/PORT LINK STATUS CHANGE:- 1 -
Trap 1.3.6.1.6.3.1.1.5.4: portIndex is 4227626, ifAdminStatus is 1,
ifOperStatus is 1

%Apr  2 00:05:27:980 2000 4500 L2INF/5/PORT LINK STATUS CHANGE:- 1 -
Ethernet1/0/1: is UP

%Apr  2 00:05:28:96 2000 4500 L2INF/5/VLANIF LINK STATUS CHANGE:- 1 -
Vlan-interface1: is UP
```

```
%Apr  2 00:05:28:213 2000 4500 STP/2/SPEED:- 1 -Ethernet1/0/1's
speed changed

!

%Apr  2 00:05:28:319 2000 4500 STP/2/PFWD:- 1 -Ethernet1/0/1 is
forwarding!

[4500-Vlan-interface2]
```

vlan

Syntax

vlan *vlan_id*

undo vlan *vlan_id* { [to *vlan_id*] | **all }**

View

System View

Parameter

vlan_id: Enter the ID of the VLAN you want to configure, in the range 1 to 4094.

all: Delete all VLANs.

Description

Use the ***vlan*** command to enter the VLAN view, and use the related configuration commands. Use the ***undo vlan*** command to exit from the specified VLAN. VLAN 1 is default VLAN and cannot be deleted.

Related commands: **display vlan**.

Example

To enter VLAN 1 view, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]vlan 1
```

Voice VLAN Configuration Commands

This section describes the commands you can use to configure voice VLANs.

display voice vlan oui

Syntax

display voice vlan oui

View

Any view

Parameter

None

Description

Use the display voice vlan oui command to display the OUI address supported by the current system and its relative features.

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

Example

To display the OUI address of Voice VLAN, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]display voice vlan oui

Oui Address               Mask              Description
00e0-bb00-0000        ffff-ff00-0000        3com phone
0003-6b00-0000        ffff-ff00-0000        Cisco phone
00e0-7500-0000        ffff-ff00-0000        Polycom phone
00d0-1e00-0000        ffff-ff00-0000        Pingtel phone
00aa-bb00-0000        ffff-ff00-0000        ABC
```

display voice vlan status

Syntax

display voice vlan status

View

Any view

Parameter

None

Description

Use the **display voice vlan status** command to display the relative Voice VLAN features including the Voice VLAN status, the configuration mode, the current Voice VLAN port status etc.

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

Example

To enable the Voice VLAN on VLAN 2 and display the Voice VLAN status, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]display voice vlan status
Voice Vlan status: ENABLE
Voice Vlan ID: 2
Voice Vlan configuration mode: AUTO
Voice Vlan security mode: Security
Voice Vlan aging time: 100 minutes
Current  voice vlan enabled port:
--------------------------------
Ethernet1/0/2, Ethernet1/0/3,
```

voice vlan aging

Syntax

voice vlan aging *minutes*

undo voice vlan aging

View

System View

Parameter

minutes: The aging time of Voice VLAN, in minutes, ranging from 5 to 43200. The default value is 1440 minutes.

Description

Use the **voice vlan aging** command to set the aging time of Voice VLAN. Use the **undo voice vlan aging** command to set the aging time back to the default.

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

Example

To set the aging time of Voice VLAN to 100 minutes, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]voice vlan aging 100
[4500]
```

voice vlan enable

Syntax

voice vlan enable

undo voice vlan enable

View

Ethernet Port View

Parameter

None

Description

Use the **voice vlan enable** command to enable the Voice VLAN features on the port. Use the **undo voice vlan enable** command to disable the Voice VLAN features on the port.

You can only run the Voice VLAN function on the port when all the Voice VLAN features in system view and port view are enabled.

For the related command, see **display voice vlan status**.

Example

To enable the Voice VLAN features on port Ethernet1/0/2, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface ethernet1/0/2
```

```
[4500-Ethernet1/0/2]voice vlan enable
[4500-Ethernet1/0/2]
```

voice vlan

Syntax

voice vlan *vlan_id* enable

undo voice vlan enable

View

System View

Parameter

vlan_id: The VLAN ID for the Voice VLAN to be enabled, in the range of 2 to 4094.

Description

Use the **voice vlan** command to globally enable the Voice VLAN features of one VLAN. Use the **undo voice vlan enable** command to globally disable the Voice VLAN features of one VLAN.

A specified VLAN must exist for a successful Voice VLAN enabling. You cannot delete a specified VLAN that has enabled Voice VLAN and only one VLAN can enable Voice VLAN features at one time.

For the related command, see **display voice vlan status**.

Example

Enable the Voice VLAN features on VLAN 2 (VLAN 2 already exists).

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]vlan 2
[4500-vlan2]quit
[4500]voice vlan 2 enable
[4500]
```

voice vlan mac_address

Syntax

voice vlan *mac_address oui* mask *oui_mask* [*description string*]

undo voice vlan mac_address *oui*

View

System View

Parameter

oui: The MAC address to be set, in the format H-H-H.

oui_mask: The valid length of a MAC address, represented by a mask, and in the format H-H-H.

description string: Description of the MAC address, in the range of 1 to 30.

Description

Use the **voice vlan *mac_address*** command to set the MAC address that the Voice VLAN can control. Use the **undo voice vlan mac_address** command to cancel this MAC address.

Here the OUI address refers to a vendor and you need only input the first three-byte values of the MAC address. The OUI address system can learn 16 MAC addresses at most. There are four default OUI addresses after the system starts:

Table 8 Default OUI Addresses

No.	OUI	Description
1	00:E0:BB	3Com phone
2	00:03:6B	Cisco phone
3	00:E0:75	Polycom phone
4	00:D0:1E	Pingtel phone

For the related command, see **display voice vlan oui**.

Example

To set the MAC address 00AA-BB00-0000 as an OUI address, enter the following.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]voice vlan mac_address 00aa-bb00-0000 mask ffff-ff00-0000
description ABC
[4500]
```

voice vlan mode

Syntax

voice vlan mode auto

undo voice vlan mode auto

View

System View

Parameter

None

Description

Use the **voice vlan mode auto** command to set the Voice VLAN in auto mode. Use the **undo voice vlan mode auto** command to set the Voice VLAN in manual mode.

By default, the Voice VLAN is in auto mode.

If required, the **voice vlan mode auto** and **undo voice vlan mode auto** commands must be executed before the Voice VLAN features are enabled globally.

For the related command, see **display voice vlan status**.

Example

To set the Voice VLAN in manual mode, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]undo voice vlan mode auto
Can't change voice vlan configuration when voice vlan is running
[4500]undo voice vlan enable
[4500]undo voice vlan mode auto
[4500]
```

voice vlan security enable

Syntax

voice vlan security enable

undo voice vlan security enable

View

System View

Parameter

None

Description

Use the **voice vlan security enable** command to enable the Voice VLAN security mode. In this mode, the system can filter out the traffic whose source MAC is not OUI when the traffic travels through the access port of IP Phone within the Voice VLAN, while the other VLANs are not influenced. Use the **undo voice vlan security enable** command to disable the Voice VLAN security mode.

By default, the Voice VLAN security mode is enabled.

If needed, the **voice vlan security enable** and **undo voice vlan security enable** commands must be executed before the Voice VLAN features are enabled globally.

For the related command, see **display voice vlan status**.

Example

To disable the Voice VLAN security mode, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]undo voice vlan security enable
[4500]
```

4 USING POWER OVER ETHERNET (POE) COMMANDS

This chapter describes how to use the following commands:

PoE Configuration Commands

PoE Configuration Commands

This section describes the commands you can use to configure and manage the PoE on your Switch 4500 PWR.

display poe interface

Syntax

display poe interface [***interface-name*** | ***interface-type interface-num*** **]**

View

Any view

Parameter

interface-name | ***interface-type interface-num:*** Port on the Switch.

Description

Use the **display poe interface** command to view the PoE status of a specific port or all ports on the Switch.

Example

Display the PoE status of the Ethernet port Ethernet1/0/10.

```
[4500]display poe interface ethernet1/0/10
Port power enabled           :enable
Port power ON/OFF            :on
Port power status            :Standard PD
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
```

Display the PoE status of all ports.

```
[4500]display poe interface

PORT INDEX      POWER         ENABLE   MODE  PRIORITY    STATUS
Ethernet1/0/1   off           enable  signal  low      Detection
Ethernet1/0/2   off           enable  signal  low      Detection
Ethernet1/0/3   off           enable  signal  low      Detection
Ethernet1/0/4   off           enable  signal  low      Detection
Ethernet1/0/5   off           enable  signal  low      Detection
Ethernet1/0/6   off           enable  signal  low      Detection
Ethernet1/0/7   off           enable  signal  low      Detection
Ethernet1/0/8   off           enable  signal  low      Detection
Ethernet1/0/9   off           enable  signal  low      Detection
Ethernet1/0/10  off           enable  signal  low      Detection
Ethernet1/0/11  off           enable  signal  low      Detection
Ethernet1/0/12  off           enable  signal  low      Detection
Ethernet1/0/13  off           enable  signal  low      Detection
Ethernet1/0/14  off           enable  signal  low      Detection
```

```
Ethernet1/0/15  off  enable  signal  low      Detection
Ethernet1/0/16  off  enable  signal  low      Detection
Ethernet1/0/17  off  enable  signal  low      Detection
Ethernet1/0/18  off  enable  signal  low      Detection
Ethernet1/0/19  off  enable  signal  low      Detection
Ethernet1/0/20  off  enable  signal  low      Detection
Ethernet1/0/21  off  enable  signal  low      Detection
Ethernet1/0/22  off  enable  signal  low      Detection
Ethernet1/0/23  off  enable  signal  low      Detection
Ethernet1/0/24  off  enable  signal  low      Detection
Ethernet1/0/25  off  disable signal  low      User set off
Ethernet1/0/26  off  disable signal  low      User set off
Ethernet1/0/27  off  disable signal  low      User set off
Ethernet1/0/28  off  disable signal  low      User set off
Ethernet1/0/29  off  disable signal  low      User set off
Ethernet1/0/30  off  disable signal  low      User set off
Ethernet1/0/31  off  disable signal  low      User set off
Ethernet1/0/32  off  disable signal  low      User set off
Ethernet1/0/33  off  disable signal  low      User set off
Ethernet1/0/34  off  disable signal  low      User set off
Ethernet1/0/35  off  disable signal  low      User set off
Ethernet1/0/36  off  disable signal  low      User set off
Ethernet1/0/37  off  disable signal  low      User set off
Ethernet1/0/38  off  disable signal  low      User set off
Ethernet1/0/39  off  disable signal  low      User set off
Ethernet1/0/40  off  disable signal  low      User set off
Ethernet1/0/41  off  disable signal  low      User set off
Ethernet1/0/42  off  disable signal  low      User set off
Ethernet1/0/43  off  disable signal  low      User set off
Ethernet1/0/44  off  disable signal  low      User set off
Ethernet1/0/45  off  disable signal  low      User set off
Ethernet1/0/46  off  disable signal  low      User set off
Ethernet1/0/47  off  disable signal  low      User set off
Ethernet1/0/48  off  disable signal  low      User set off
```

display poe power

Syntax

display poe interface power [***interface-name*** | ***interface-type interface-num*** **]**

View

Any view

Parameter

interface-name | ***interface-type interface-num:*** Port on the Switch.

Description

Use the **display poe interface power** command, you can view the power information of a specific port or all ports on the Switch.

Example

Display the power information of port Ethernet1/0/10.

```
[4500]display poe interface power ethernet1/0/10
```

```
Port power                    :12400 mW
```

Display the power information of all ports.

```
[4500]display poe power
PORT INDEX                              POWER (mW)   PORT    INDEXPOWER
(mW)
Ethernet1/0/1                           0
Ethernet1/0/2                           100
Ethernet1/0/3                           200
Ethernet1/0/4                           300
Ethernet1/0/5                           400
Ethernet1/0/6                           500
Ethernet1/0/7                           600
Ethernet1/0/8                           700
Ethernet1/0/9                           800
Ethernet1/0/10                          900
Ethernet1/0/11                          1000
Ethernet1/0/12                          1100
Ethernet1/0/13                          1200
Ethernet1/0/14                          1300
Ethernet1/0/15                          1400
Ethernet1/0/16                          1500
Ethernet1/0/17                          1600
Ethernet1/0/18                          1700
Ethernet1/0/19                          1800
Ethernet1/0/20                          1900
Ethernet1/0/21                          2000
Ethernet1/0/22                          2100
Ethernet1/0/23                          2200
Ethernet1/0/24                          2300
Ethernet1/0/25                          2400
Ethernet1/0/26                          2500
Ethernet1/0/27                          2600
Ethernet1/0/28                          2700
Ethernet1/0/29                          0
Ethernet1/0/30                          0
Ethernet1/0/31                          0
Ethernet1/0/32                          0
Ethernet1/0/33                          3200
Ethernet1/0/34                          3300
Ethernet1/0/35                          3400
Ethernet1/0/36                          3500
Ethernet1/0/37                          3600
Ethernet1/0/38                          3700
Ethernet1/0/39                          3800
Ethernet1/0/40                          3900
Ethernet1/0/41                          4000
Ethernet1/0/42                          4100
Ethernet1/0/43                          4200
Ethernet1/0/44                          4300
Ethernet1/0/45                          4400
Ethernet1/0/46                          4500
Ethernet1/0/47                          4600
Ethernet1/0/48                          4700
```

display poe powersupply

Syntax

display poe powersupply

View

Any view

Parameter

None

Description

Use the **display poe powersupply** command to view the parameters of the power sourcing equipment (PSE).

Example

Display the PSE parameters.

```
[4500]display poe powersupply

PSE ID                       :1
PSE Legacy Detection         :disable
PSE Total Power Consumption :12000 mW
PSE Available Power          :268000 mW
PSE Peak Value               :12000 mW
PSE Average Value            :12000 mW
PSE Software Version         :290
PSE Hardware Version         :000
PSE CPLD Version             :021
PSE Power-Management mode    :auto
```

poe enable

Syntax

poe enable

undo poe enable

View

Ethernet Port View

Parameter

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 each port is enabled.

Example

Enable the PoE feature on the current port.

```
[4500-Ethernet1/0/3]poe enable
Port power supply is enabled
# Disable the PoE feature on the current port.
[4500-Ethernet1/0/3]undo poe enable
Port power supply is disabled
```

poe legacy enable

Syntax

poe legacy enable

undo poe legacy enable

View

System View

Parameter

None

Description

Use the **poe legacy enable** command to enable the nonstandard-PD detect function.

Use the **undo poe legacy enable** command to disable the nonstandard-PD detect function.

PDs compliant with 802.3af standards are called standard PDs.

By default, the nonstandard-PD detect function is disabled.

Example

Enable the nonstandard-PD detect function.

```
[4500]poe legacy enable
Legacy detection is enabled
```

Disable the nonstandard-PD detect function.

```
[4500]undo poe legacy enable
Legacy detection is disabled
```

poe max-power

Syntax

poe max-power ***max-power***

undo poe max-power

View

Ethernet Port View

Parameter

max-power: Maximum power distributed to the port, ranging from 1000 to 15400 mW.

Description

Use the **poe max-power** command to configure the maximum power that can be supplied by current port.

Use the **undo poe max-power** command to restore the maximum power supplied by current port to the default value.

By default, the maximum power that a port can supply is 15400 mW.

The unit of power is mW. 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.

Example

Set the maximum power supplied by current port.

```
[4500-Ethernet1/0/3]poe max-power 15000
Set Port max power successfully
```

Restore the default maximum power on the current port.

```
[4500-Ethernet1/0/3]undo poe max-power
Set Port max power successfully
```

poe mode

Syntax

poe mode { signal | spare }

undo poe mode

View

Ethernet Port View

Parameter

signal: Supply power through the signal line.

spare: Supply power through the spare line. Currently, the Switch 4500 Family does not support **spare** mode. If the subordinate PD only supports the **spare** mode, a conversion is needed.

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, the port is powered through the signal cable.

Example

Set the PoE mode on current port to *signal*.

```
[4500-Ethernet1/0/3]poe mode signal
Set PoE mode successfully
```

poe power-management

Syntax

poe power-management { auto | manual }

undo poe power-management

View

System View

Parameter

auto: Adopt the **auto** mode, a PoE management mode based on port priority.

manual: Adopt 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***.

Example

Configure the PoE management mode on port to auto.

```
[4500]poe power-management auto
Auto Power Management is enabled
```

Restore the default management mode.

```
[4500]undo poe power-management
Auto Power Management is enabled
```

poe priority

Syntax

poe priority { *critical* | *high* | *low* }

undo poe priority

View

Ethernet Port View

Parameter

critical: Set the port priority to ***critical***.

high: Set the port priority to ***high***.

low: Set the port priority to ***low***.

Description

Use the **poe priority** command to configure the power supply priority on a port.

Use the **undo poe priority** command to restore the default priority.

By default, the port priority is **low**.

If there are too many ports with critical priority, the total power these ports need might exceed the maximum power supplied by the equipment, i.e., 300W. In this case, no new PD can be added to the switch.

When the remaining power of the whole equipment is below 18.8 W, no new PD can be added to the Switch.

Example

Set the port priority to **critical**.

```
[4500-Ethernet1/0/3]poe priority critical
```

Set Port POE priority successfully

Restore the default priority.

```
[4500-Ethernet1/0/3]undo poe priority
Set Port POE priority successfully
```

poe update

Syntax

poe update { refresh | **full }** ***filename***

View

System View

Parameter

refresh: The refresh update mode is used when the PSE processing software is valid.

full: The full update mode is used when the PSE has no valid processing software.

filename: Update file name, with a length of 1 to 64 characters.

Description

Use the **poe update** command to update the PSE processing software online

Note that:

- The full mode is used only when you cannot use the **refresh** mode.
- When the update procedure in **refresh** mode is interrupted for some unexpected reason (e.g. power-off) or some errors occur, you can use the **full** mode to re-update.
- 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.

Example

Update the PSE processing software online.

```
[4500]poe update refresh 0290_021.s19
.................................................................
.................................................................
.................................................................
.................................................................
.................................................................
.................................................................
.................................................................
.................................................................
.................................................................
...........
Update PoE board successfully
```

5 USING NETWORK PROTOCOL COMMANDS

This chapter describes how to use the following commands:

IP Address Configuration Commands

- display ip host
- display ip interface vlan
- ip address
- ip host

ARP Configuration Commands

- arp check enable
- arp static
- arp static
- debugging arp packet
- display arp
- display arp timer aging
- reset arp

DHCP Client Configuration Commands

- debugging dhcp client
- debugging dhcp xrn xha
- display dhcp client
- ip address dhcp-alloc

DHCP Relay Configuration Commands

- debugging dhcp-relay
- dhcp-server
- dhcp-server ip
- display dhcp-server
- display dhcp-server interface vlan-interface

Access Management Configuration Commands

- am enable
- am ip-pool
- am trap enable
- display am

- display isolate port
- port isolate

UDP Helper Configuration Commands

- debugging udp-helper
- display udp-helper server
- udp-helper enable
- udp-helper port
- udp-helper server

IP Performance Configuration Commands

- display fib
- display fib ip_address
- display fib acl
- display fib
- display fib ip-prefix
- display fib statistics
- display icmp statistics
- display ip socket
- display ip statistics
- display tcp statistics
- display tcp status
- display udp statistics
- reset ip statistics
- reset tcp statistics
- reset udp statistics
- tcp timer fin-timeout
- tcp timer syn-timeout
- tcp window

IP Address Configuration Commands

This section describes the commands you can use to configure and manage IP Addressing on your Switch 4500.

display ip host

Syntax

display ip host

View

All views

Parameter

None

Description

Use the **display ip host** command to display all host names and their corresponding IP addresses.

Example

To display all host names and their corresponding IP addresses, type the following:

```
<4500>display ip host
```

The information displays in the following format:

```
Host     Age   Flags   Address
My       0     static  1.1.1.1
Aa       0     static  2.2.2.4
```

display ip interface vlan

Syntax

display ip interface *interface-type interface-num*

View

All views

Parameter

interface-type Enter the port type.

interface-num Enter the port number.

Related commands: **interface**

Description

Use the **display ip interface** command to view information on the specified interface.

Example

To display information for VLAN-interface 1, enter the following:

```
<4500>display ip interface vlan-interface 1
```

The information displays in the following format:

```
Vlan-interface1 current state : DOWN
```

```
Line protocol current state : DOWN
Internet Address is 1.1.1.1/8 Primary
Broadcast address : 1.255.255.255
The Maximum Transmit Unit : 1500 bytes
input packets : 0, bytes : 0, multicasts : 0
output packets : 0, bytes : 0, multicasts : 0
TTL invalid packet number:         0
ICMP packet input number:          0
  Echo reply:                      0
  Unreachable:                     0
  Source quench:                   0
  Routing redirect:                0
  Echo request:                    0
  Router advert:                   0
  Router solicit:                  0
  Time exceed:                     0
  IP header bad:                   0
  Timestamp request:               0
  Timestamp reply:                 0
  Information request:             0
  Information reply:               0
  Netmask request:                 0
  Netmask reply:                   0
  Unknown type:                    0
DHCP packet deal mode:  global
```

ip address

Syntax

ip address ***ip_address*** { ***mask*** | ***mask_length*** }

[undo] ip address [***ip-address*** { ***mask*** | ***mask_length*** }]

View

VLAN Interface view

Parameters

ip_address Enter the IP address of the VLAN interface.

mask Enter the IP subnet mask of the VLAN interface.

mask_length Enter the IP mask length of the VLAN interface.

Description

Use the **ip address** command to configure the IP address for a VLAN interface.

Use the **undo ip address** command to cancel an IP address for a VLAN interface.

By default, the IP address of a VLAN interface is set to null.

Related commands: **display ip interface**.

Example

Configure the IP address of interface VLAN interface 1 as 202.38.10.66.

```
[4500-vlan-interface1]ip address 202.38.10.66
```

ip host

Syntax

ip host *hostname ip_address*

undo ip host *hostname* [*ip_address*]

View

System view

Parameters

hostname Enter the host name of the connecting device. This is a character string of up to 20 characters.

ip_address Enter the host's IP address.

Description

Use the **ip host** command to configure the host name and the host IP address in the Switch 4500's host table. This allows you to ping or Telnet a local device by host name.

Use the **undo ip host** command to remove the host name and the host IP address from the host table.

By default, the host name and corresponding IP address are null.

Related command: **display ip host**

Example

To enter a host name of Lanswitch1 for the IP address 202.38.0.8, enter the following.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]ip host Lanswitch1 202.38.0.8
```

ARP Configuration Commands

This section describes the commands you can use to configure and manage the Address Resolution Protocol (ARP) operations on your Switch 4500.

arp check enable

Syntax

arp check enable

undo arp check enable

View

System View

Parameter

none

Description

Use the **arp check enable** command to enable the checking of an ARP entry so the device does not learn the ARP entry where the MAC address is a multicast

MAC address. Use the **undo arp check enable** command to disable the checking of ARP entry so the device learns the ARP entry where the MAC address is a multicast MAC address.

By default, the checking of ARP entry is enabled and the device does not learn the ARP entry where the MAC address is a multicast MAC address.

Example

Configure that the device learns the ARP entry where the MAC address is multicast MAC address.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]undo arp check enable
```

arp static

Syntax

arp static ***ip_address mac_address*** **[** ***vlan_id*** **{** ***interface_type*** | ***interface_number*** **}]**

undo arp static ***ip_address***

View

System View

Parameters

ip_address Enter the IP address of the ARP mapping entry.

mac_address Enter the MAC address of the ARP mapping entry, in the format H-H-H (H indicates a four digit hexadecimal number, for example 00e0-fc01-0000).

vlan_id Enter the ID number of the local VLAN that you want to use to associate with the ARP mapping entry. The VLAN ID can be in the range 1 to 4094. Optional.

interface_type Enter the type of the port that you want to use to send frames to this address. Optional, but must be entered if a VLAN ID is specified.

interface_number Enter the number of the port that you want to use to send frames to this address. Optional, but must be entered if a VLAN ID is specified.

Description

Use the **arp static** command to manually configure the static ARP mapping entries in the ARP mapping table. You must enter an IP address and MAC address with this command. You can optionally enter a VLAN ID, which also requires entry of an interface type and interface number. An aggregation port or port with LACP enabled cannot be set as the egress port of static ARP.

Use the **undo arp** *ip_address* command to remove a static ARP mapping entry from the ARP table.

To remove all static ARP entries, use the **reset arp static** *command. Note that the* **reset arp static** *command removes all static ARP entries permanently.*

By default, the ARP mapping table is empty, and the Switch uses dynamic ARP to maintain its address mapping.

Related commands: **reset arp**, **display arp**, **debugging arp**.

Example

To associate the IP address 202.38.10.2 with the MAC address 00e0-fc01-0000, and the ARP mapping entry to Ethernet1/0/1 on VLAN1, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]arp static 202.38.0.10 00e0-fc01-0000 1 Ethernet1/0/1
```

arp static

Note that this command does the same as the command above, except there is no port parameter as you are already in the port view.

Syntax

arp static ***ip_address mac_address vlan_id***
undo arp static ***ip_address***

View

Ethernet Port View

Parameters

ip_address Enter the IP address of the ARP mapping entry.

mac_address Enter the MAC address of the ARP mapping entry, in the format H-H-H (H indicates a four digit hexadecimal number, for example 00e0-fc01-0000).

vlan_id Enter the ID number of the VLAN that you want to use to associate with the ARP mapping entry.

The VLAN ID can be in the range 1 to 4094. Optional.

Description

Use the **arp static** command to manually configure the static ARP mapping entries in the ARP mapping table. You must enter an IP address and MAC address with this command. You can optionally enter a VLAN ID.

Use the **undo arp static** *ip_address* command to remove a static ARP mapping entry from the ARP table.

To remove all static ARP entries, use the **reset arp static** *command. Note that the* **reset arp static** *command removes all static ARP entries permanently.*

By default, the ARP mapping table is empty, and the Switch uses dynamic ARP to maintain its address mapping.

Related commands: **reset arp**, **display arp**, **debugging arp**.

Example

To establish a mapping between IP address 129.102.0.1 and MAC address 00e0-fc01-0000, and to send frames to this address through VLAN 1, Ethernet port 1/0/1, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]arp static 202.38.0.10 00e0-fc01-0000 1 arp timer aging
```

Syntax

arp timer aging *aging_time*

undo arp timer aging

View

System View

Parameter

aging_time Enter the aging time of dynamic ARP aging timer, in the range 1 to 1440 minutes. The default is 20 minutes.

Description

Use the **arp timer aging** command to configure the dynamic ARP aging timer.

Use the **undo arp timer aging** command to restore the default time of 20 minutes.

Related commands: **display arp timer aging**

Example

To configure the dynamic ARP aging timer to 10 minutes, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]arp timer aging 10
```

debugging arp packet

Syntax

debugging arp [packet | **error** | **info packet]**

undo debugging arp packet

View

User View

Parameters

error Enter to enable ARP error debugging.

info Enter to enable ARP mapping table and information management debugging.

packet Enter to enable ARP packet debugging.

Description

Use the **debugging arp** command to enable ARP debugging.

Use the **undo debugging arp** command to disable the corresponding ARP debugging.

By default, undo ARP debugging is enabled.

For the related commands, see **arp static** and **display arp**.

Example

To enable ARP packet debugging, enter the following:

```
<4500>debugging arp packet

*0.771346-ARP-8-S1-arp_send:Send an ARP Packet, operation : 1,
sender_eth_addr :

 00e0-fc00-3500,sender_ip_addr : 10.110.91.159, target_eth_addr :
0000-0000-0000

, target_ip_addr : 10.110.91.193

*0.771584-ARP-8-S1-arp_rcv:Receive an ARP Packet, operation : 2,
sender_eth_addr

 : 0050-ba22-6fd7, sender_ip_addr : 10.110.91.193, target_eth_addr :
00e0-fc00-3500, target_ip_addr : 10.110.91.159
```

Table 9 Output Description of the **debugging arp packet** Command

Field	Description
operation	Type of ARP packets: 1 ARP request packet; 2 ARP reply packet
sender_eth_addr	Ethernet address of the sender
sender_ip_addr	IP address of the sender
target_eth_addr	Target Ethernet address. If the packet is ARP request packet, the target IP address will be 0
target_ip_addr	Target IP address

display arp

Syntax

display arp [***ip-address*** | **[dynamic** | **static] [** | **{ begin** | **include** | **exclude } *text*]]**

View

All views

Parameters

dynamic: Enter to display the dynamic ARP entries in the ARP mapping table.

static: Enter to display the static ARP entries in the ARP mapping table.

begin: Enter to start displaying from the first ARP entry that contains the specified character string "text".

include: Enter to display only the ARP entries that contain the specified character string "text".

exclude: Enter to display only the ARP entries that do not contain the specified character string "text".

text Enter a character string. The ARP entries that contain this character string are displayed.

Description

Use the **display arp** command to display the ARP mapping table entries by entry type, or by a specified IP address.

Related commands: **arp static**, **reset arp**.

Example

To display all ARP entries in the mapping table, enter the following:

```
<4500>display arp
Type: S-Static   D-Dynamic
IP Address    MAC Address     VLAN ID  Port Name / AL ID Aging Type
161.71.61.20 0012-1212-1213 1         Aggregation Link 1    20    D

---   1 entry found   ---
<4500>
```

Table 10 Output Description of the **display arp** Command

Field	Description
IP Address	IP address of the ARP mapping entry
MAC Address	MAC address of the ARP mapping entry
VLAN ID/ AL ID	VLAN to which the static ARP entry belongs
Port Name	Port to which the static ARP entry belongs
Aging	Aging time of dynamic ARP entry in minutes
Type	Type of ARP entry

display arp timer aging

Syntax

display arp timer aging

View

All views.

Parameter

None.

Description

Use the **display arp timer aging** command to view the current setting of the dynamic ARP aging timer.

Example

To display the current setting of the dynamic ARP aging timer, enter the following:

```
<4500>system-view
```

```
System View: return to User View with Ctrl+Z.
[4500] display arp timer aging
```

The information displays in the following format:

```
Current ARP aging time is 20 minute(s) (default)
[4500]
```

reset arp

Syntax

reset arp [dynamic | **static** | **interface { *interface_type interface_num*** | ***interface_name* }]**

View

User view

Parameters

dynamic Enter to clear the dynamic ARP mapping entries. Note that dynamic ARP entries start re-learning immediately.

static Enter to clear the static ARP mapping entries. Note that static ARP entries are deleted permanently.

interface *interface_type interface_num interface_name* Enter to clear the ARP mapping entries for the specified port.

Description

Use the **reset arp** command to remove information that is no longer required from the ARP mapping table. You can remove entries of a specified type, or from a specified port.

Use the **reset arp** command to clear all ARP entries. You are asked to confirm this entry.

Use the **reset arp dynamic** command to clear all dynamic ARP entries.

Use the **reset arp static** command to clear all static ARP entries.

Use the **display arp interface** command to clear all entries for the specified port.

Related command: **arp static**, **display arp**.

Example

To clear static ARP entries, enter the following:

```
<4500>reset arp static
```

DHCP Client Configuration Commands

This section describes the commands you can use to configure and manage the Dynamic Host Configuration Protocol (DHCP) Client operations on your Switch 4500.

debugging dhcp client

Syntax

debugging dhcp client { all | **error** | **event** | **packet }**

undo debugging dhcp client { all | **error** | **event** | **packet }**

View

User view

Parameters

all Enter to enable all DHCP client debugging.

error Enter to enable DHCP client error (including packet unrecognizable) debugging.

event Enter to enable DHCP client event (including address allocation and data update) debugging.

packet Enter to enable DHCP client packet debugging.

Description

Use the **debugging dhcp client** command to enable DHCP client debugging.

Use the u**ndo debugging dhcp client** command to disable DHCP client debugging.

By default, DHCP client debugging is disabled.

Example

To enable DHCP client event debugging, enter the following:

<4500>**debugging dhcp client event**

debugging dhcp xrn xha

Syntax

debugging dhcp xrn xha

undo debugging dhcp xrn xha

View

User view

Parameter

None

Description

Use the **debugging dhcp xrn xha** command to enable DHCP client hot backup debugging.

Use the **undo debugging dhcp xrn xha** command to disable DHCP client hot backup debugging.

By default, DHCP client hot backup debugging is disabled.

Example

To enable DHCP client hot backup debugging, enter the following:

```
<4500>debugging dhcp xrn xha
```

display dhcp client

Syntax

display dhcp client [verbose]

View

Any view

Parameter

verbose Enter to display detailed information about address allocation at DHCP client.

Description

Use the **display dhcp client** command to view detailed information about address allocation at DHCP client.

Example

To display detailed information about address allocation at DHCP client, enter the following:

```
<4500>display dhcp client verbose
DHCP client statistic information:
Vlan-interface1:
Current machine state: BOUND
Alloced IP: 169.254.0.2 255.255.0.0
Alloced 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: 169.254.0.1
Transaction ID = 0x3d8a7431
Default router: 2.2.2.2
DNS server: 1.1.1.1
Domain name: 3Com.com
Client ID: 3com-00e0.fc0a.c3ef-Ethernet0/0
Next timeout will happen after 0 days 11 hours 56 minutes 1 seconds.
```

ip address dhcp-alloc

Syntax

ip address dhcp-alloc

undo ip address dhcp-alloc

View

VLAN Interface View

Parameter

None

Description

Use the ip address dhcp-alloc command to configure VLAN interface to obtain IP address using DHCP.

Use the undo ip address dhcp-alloc command to remove the configuration.

By default, the VLAN interface does not obtain an IP address using DHCP.

Example

To configure VLAN interface to obtain IP address using DHCP, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface vlan-interface 1
[4500-Vlan-interface1]ip address dhcp-alloc
```

DHCP Relay Configuration Commands

This section describes the commands you can use to configure and manage the Dynamic Host Configuration Protocol (DHCP) operations on your Switch 4500.

debugging dhcp-relay

Syntax

debugging dhcp-relay

undo debugging dhcp-relay

View

User view

Parameter

None

Description

Use the **debugging dhcp-relay** command to enable DHCP relay debugging.

Use the **undo debugging dhcp-relay** command to disable DHCP relay debugging. By default, DHCP relay debugging is disabled.

Related commands: **dhcp-server ip**, **dhcp-server**, **display dhcp-server** and display **dhcp-server interface vlan-interface**.

Example

To enable DHCP relay debugging, enter the following:

```
<4500>debugging dhcp-relay
*0.7200205-DHCP-8-dhcp_debug:
From client to server:
Interface: VLAN-Interface 1
ServerGroupNo: 0
```

```
Type: dhcp-request
ClientHardAddress: 0010-dc19-695d
          ServerIpAddress: 192.168.1.2

*0.7200230-DHCP-8-dhcp_debug:
From server to client:
Interface: VLAN-Interface 1
ServerGroupNo: 0
Type: dhcp-ack
ClientHardAddress: 0010-dc19-695d
         AllocatedIpAddress: 10.1.1.1

*0.7200580-DHCP-8-largehop:
Discard DHCP request packet because of too large hop count!

*0.7200725-DHCP-8-invalidpkt:
Wrong DHCP packet!
```

dhcp-server

Syntax

dhcp-server *groupNo*

undo dhcp-server

View

VLAN Interface View

Parameter

groupNo Enter the DHCP Server group number, in the range 0 to 19.

Description

Use the **dhcp-server** command to associate a VLAN interface with a DHCP Server group. DHCP Server requests are forward to the server associated with this group from the specified interface.

Use the **undo dhcp-server** command to remove the VLAN interface from the selected DHCP Server group. By default, DHCP Server requests are not forwarded.

You can only add the primary VLAN interface to a DHCP Server group. The primary VLAN interface is the first interface that you configure.

This command has more parameters when entered in system view. Refer to **dhcp-server ip** *below for details.*

Related commands: **dhcp-server ip**, **display dhcp-server**, **display dhcp-server interface vlan-interface, debugging dhcp-relay**.

Example

To add VLAN-Interface 1 to DHCP Server group1, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface vlan-interface 1
[4500-Vlan-interface1]dhcp-server 1
```

dhcp-server ip

Syntax

dhcp-server *groupNo* ip *ipaddress1* [*ipaddress2*]

undo dhcp-server *groupNo*

View

System View

Parameters

groupNo Enter the DHCP server group number, in the range 0 to 19.

ip_address1 Enter the IP address of the primary Server in the group.

ip_address2 Enter the IP address of the secondary Server in the group. Optional.

Description

Use the **dhcp-server ip** command to configure the IP address of the DHCP Server used by the DHCP Server group.

Use the **undo dhcp-server ip** command to delete the IP addresses of all DHCP Servers in DHCP Server group.

*This command has fewer parameters when entered in VLAN Interface View. Refer to **dhcp-server** command for details.*

Related commands: **dhcp-server**, **debugging dhcp-relay**.

Example

To configure the primary and secondary IP addresses of DHCP Server group 1 as 1.1.1.1 and 2.2.2.2 respectively, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]dhcp-server 1 ip 1.1.1.1 2.2.2.2
```

To delete the IP addresses of DHCP Server group1, enter the following:

```
[4500]undo dhcp-server 1
```

display dhcp-server

Syntax

display dhcp-server *groupNo*

View

All views.

Parameter

groupNo Enter a DHCP Server group number, in the range 0 to 19.

Description

Use the **display dhcp-server** command to view information on a selected DHCP Server group.

Related commands: **dhcp-server ip**, **dhcp-server**, **display dhcp-server interface vlan-interface**, **debugging dhcp-relay**.

Example

To view information on DHCP Server group 0, enter the following:

```
<4500>display dhcp-server 0
```

The information displays in the following format:

```
The first IP address of DHCP Server group 0: 1.1.1.1
The second IP address of DHCP Server group 0: 1.1.1.2
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
```

display dhcp-server interface vlan-interface

Syntax

display dhcp-server interface vlan-interface *vlan_id*

Views

All views

Parameter

vlan_id Enter the VLAN interface number.

Description

Use the **display dhcp-server interface vlan-interface** command to display the information on the DHCP Server group corresponding to a specific VLAN interface.

Related commands: **dhcp-server**, **display dhcp-server**, **debugging dhcp-relay**.

Example

To view the information on the DHCP Server group corresponding to VLAN-Interface 2, enter the following:

```
<4500>display dhcp-server interface vlan-interface 2
```

The information displays in the following format:

```
The DHCP server group of this interface is 0
```

The information shown above indicates that vlan-interface 2 is configured with a DHCP Server group whose ID is 0.

Access Management Configuration Commands

This section describes the commands you can use to configure and manage the Access Management Configuration operations on your Switch 4500.

am enable

Syntax

am enable

undo am enable

View

System View

Parameter

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, the Access management function is disabled.

When using the access management function, It is recommended that you cancel the static ARP configuration to ensure that the binding of the IP address and Ethernet switch takes effect. If you have configured the static ARP for an IP address in the current port IP address pool from another port, the system will prompt you to cancel the static ARP setting.

Example

To enable the access management function, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]am enable
```

am ip-pool

Syntax

am ip-pool ***address-list***

undo am ip-pool { all | ***address-list*** **}**

View

Ethernet Port View

Parameters

all Enter to configure to operate on all the IP addresses (or IP address pools).

ip-pool Enter to configure IP address pool for access management.

address-list Enter IP address list in the *start_ip_address* **[***ip_address_num* **] & < 1-10 >** format.

start_ip_address Is the start address of an IP address range in the pool.

ip_address_num: Specifies how many IP addresses following *start_ip_address* in the range.

&< 1-10 > means you can specify ten IP address ranges at most.

Description

Use the **am ip-pool** command to configure the IP address pool for access management on a port. The packet whose source IP address is in the specified pool is allowed to be forwarded on Layer 3 via the port of the switch.

Use the **undo am ip-pool** command to cancel the access management IP pool of the port.

By default, all the IP address pools for access management on the port are null and all the packets are permitted through.

Note that if the IP address pool to be configured contains the IP addresses configured in the static ARP at other ports, then the system prompts you to delete the static ARP to make the later binding effective.

Example

To configure the access management IP address pool on Ethernet1/0/1 and permits the addresses from 202.112.66.2 through 202.112.66.20 and the specified 202.112.65.1 to access the port, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface ethernet 1/0/1
[4500-Ethernet1/0/1]am ip-pool 202.112.66.2 19 202.112.65.1
```

am trap enable

Syntax

am trap enable

undo am trap enable

View

System View

Parameter

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 is disabled.

Example

To enable the access management trap, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]am trap enable
```

display am

Syntax

display am [***interface-list*** **]**

View

Any view

Parameters

interface-list Enter to display the access management information of the specified port in the **{ {** ***interface_type interface_num*** | ***interface_name*** **} [** to **{** ***interface_type interface_num*** | ***interface_name*** **}] } &<1-10>** format.

interface_name Enter the port name, represented with ***interface_name***= ***interface_type interface_num***.

interface_type is the port type and ***interface_num*** is the port number.

&<1-10> indicates the preceding parameter can be input up to 10 times.

Description

Use the **display am** command to view the current access management configurations on part or all of the ports.

Use the **display am** command to view the status of access management function and configuration of IP address pool.

Example

To display the access management configurations on Ethernet0/1 and Ethernet0/2.

```
<4500>display am Ethernet0/1 Ethernet0/2
Ethernet0/1
 Status       : disabled
 IP Pools     : (NULL)
 Isolate Ports: Ethernet0/2
Ethernet0/2
 Status       : disabled
 IP Pools     : (NULL)
 Isolate Ports: Ethernet0/1
```

Table 11 Output Description of the **display am** Command

Field	Description
Status	AM state on the port: enabled or disabled
IP Pools	IP pools. NULL represents no configuration. Each IP address section is represented in X.X.X.X (number), of these, "X.X.X.X" represents the first address, and "number" represents that "number" consecutive IP addresses from the beginning of this address are within the IP pools
Isolate Ports	Isolate ports. NULL represents no configuration

To display the access management configurations on Ethernet1/0/1:

```
<4500> display am ethernet1/0/1

Ethernet1/0/1
 Status       : disabled
 IP Pools     : (NULL)
```

display isolate port

Syntax

display isolate port

View

Any view

Parameter

none

Description

Use the **display isolate port** command to view port isolation information.

Example

To display port isolation information, enter the following:

```
<4500>display isolate port
Isolated port(s) on UNIT 1:
Ethernet1/0/1
```

port isolate

Syntax

port isolate

undo port isolate

View

Ethernet Port View

Parameter

none

Description

Use the **port isolate** command to add a port to an isolation group using the following commands, and achieves port-to-port isolation between this port and

other ports of this group, that is, Layer 2 forwarding between the isolated ports is not available.

Use the **undo port isolate** command to remove a port from an isolation group.

By default, a port is not in an isolation group, namely Layer 2 forwarding is achievable between this port and other ports.

Example

To add Ethernet1/0/1 and Ethernet1/0/2 to isolation group, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface ethernet 1/0/1
[4500-Ethernet1/0/1]port isolate
[4500-Ethernet1/0/1]quit
[4500]interface ethernet 1/0/2
[4500-Ethernet1/0/2]port isolate
```

UDP Helper Configuration Commands

This section describes the commands you can use to configure and manage the UDP Helper Configuration operations on your Switch 4500.

debugging udp-helper

Syntax

debugging udp-helper { event | packet [receive | send] }

undo debugging udp-helper { event | packet [receive | send] }

View

User view

Parameters

event UDP Helper event debugging.

packet UDP Helper packet debugging.

receive UDP Helper inbound packet debugging.

send UDP Helper outbound packet debugging.

Description

Use the **debugging udp-helper** command to enable UDP Helper debugging.

Use the **undo debugging udp-helper** command to disable UDP Helper debugging.

By default, UDP Helper debugging is disabled.

Example

To enable UDP Helper packet debugging, enter the following:

```
<4500>debugging udp-helper packet
```

display udp-helper server

Syntax

display udp-helper server [interface vlan-interface *vlan_id* **]**

View

Any view

Parameter

vlan_id VLAN interface ID.

Description

Use the **display udp-helper server** command to view the information of destination Helper server corresponding to the VLAN interface.

Example

To display the information of destination Helper server corresponding to the VLAN interface 1, enter the following:

```
<4500>display udp-helper server interface vlan-interface 1

interface name   server address  packets sent
VLAN-interface1  192.1.1.2       0
```

udp-helper enable

Syntax

udp-helper enable

undo udp-helper enable

View

System View

Parameter

None

Description

Use the **udp-helper enable** command to enable the UDP Helper function.

Use the **undo udp-helper enable** command to disable the UDP Helper function.

By default, UDP Helper function is disabled.

Example

To enable the UDP Helper function.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]udp-helper enable
```

udp-helper port

Syntax

udp-helper port { *port* | dns | netbios-ds | netbios-ns | tacacs | tftp | time }

undo udp-helper port { *port* | dns | netbios-ds | netbios-ns | tacacs | tftp | time }

View

System view

Parameters

port Enter the ID of the UDP port with relay function to be enabled, in the range of 1 to 65535.

dns Domain name service, corresponding to UDP port 53.

netbios-ds NetBios datagram service, corresponding to UDP port 138.

netbios-ns NetBios name service, corresponding to UDP port 137.

tacacs TAC access control system, corresponding to UDP port 49.

tftp Trivial file transfer protocol, corresponding to UDP port 69.

time Time service, corresponding to UDP port 37.

Description

Use the **udp-helper port** command to configure the UDP port with relay function.

Use the **undo udp-helper enable** command to delete the UDP port with relay function.

Example

To configure the UDP port with relay function as the UDP port corresponding to DNS, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]udp-helper port dns
```

udp-helper server

Syntax

udp-helper server *ip-address*

undo udp-helper server [*ip-address*]

View

VLAN Interface View

Parameter

ip-address Enter the IP address of the destination server.

Description

Use the **udp-helper server** command to configure the relay destination server.

Use the **undo udp-helper server** command to delete the relay destination server.

By default, no relay destination server is configured.

Related command: **display udp-helper server**.

Example

To configure the relay destination server with IP address 192.1.1.2, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface vlan-interface 1
[4500-Vlan-interface1]udp-helper server 192.1.1.2
```

IP Performance Configuration Commands

This section describes the commands you can use to configure and manage the IP Performance Configuration operations on your Switch 4500.

display fib

Syntax

display fib

View

Any view

Parameter

none

Description

Use the **display fib** command to view the summary of the forwarding information base. The information includes: destination address/mask length, next hop, current flag, timestamp and outbound interface.

Example

To display the summary of the Forwarding Information Base, enter the following:

```
<4500>display fib
Destination/Mask    Nexthop         Flag TimeStamp     Interface
127.0.0.0/8         127.0.0.1       U    t[0]          InLoopBack0
```

Table 12 Description of the output information of the **display fib** command

Field	Description
Flag	The flag options include: B – Blackhole route D – Dynamic route G – Gateway route H – Local host route S – Static route U – Route in UP status R – Unreachable route

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 Enter destination IP address, in dotted decimal format. ***ip_address1*** and ***ip_address2*** jointly define the address range. The FIB entries in this address range will be displayed.

mask1, mask2, mask-length1, mask-length2 Enter the IP address mask, in dotted decimal format, or an integer in the range of 0 to 32 to represent the mask length.

longer All FIB entries matched in the natural mask range.

Description

Use the **display fib *ip_address*** command to view the FIB entries matching the destination IP address (range). Each line outputs a FIB entry and the display contents for each entry include destination address/mask length, next hop, current flag, timestamp and outbound interface.

Example

To display the FIB entries whose destination addresses match 169.253.0.0 in natural mask range, enter the following:

```
<4500>display fib 169.253.0.0
Route Entry Count: 1
Destination/Mask   Nexthop    Flag  TimeStamp  Interface
169.0.0.0/16       2.1.1.1    U     t[0]       Vlan-interface1
```

To display the FIB entries whose destination addresses are in the range of 169.254.0.0/16 to 169.254.0.6/16, enter the following:

```
<4500>display fib 169.254.0.0 255.255.0.0 169.254.0.6 255.255.0.0
Route Entry Count: 1
Destination/Mask   Nexthop    Flag  TimeStamp  Interface
169.254.0.1/16     2.1.1.1    U       t[0]     Vlan-interface1
```

display fib acl

Syntax

display fib acl *number*

View

Any view

Parameter

number Enter the ACL in number form, in the range 2000 to 2999

Description

Use the **display fib acl** command to view the FIB entries matching a specific ACL.

Example

To display the FIB entries matching ACL 2000, enter the following:

```
<4500>display fib acl 2000
Route entry matched by access-list 2000:
Summary counts: 1
Destination/Mask   Nexthop    Flag    TimeStamp  Interface
127.0.0.0/8        127.0.0.1  U       t[0]       InLoopBack0
```

display fib

Syntax

display fib | **{ { begin** | **include** | **exclude } text }**

View

Any view

Parameters

begin Enter to display the FIB entries from the first one containing the character string text.

include Enter to display only those FIB entries containing the character string text.

exclude Enter to display only those FIB entries excluding the character string text.

text Enter string of specific characters.

Description

Use the **display fib** command to view the FIB entries which are output from the buffer according to regular expression and related to the specific character string.

Example

To display the lines starting from the first one containing the string 169.254.0.0, enter the following:

```
<4500>display fib | begin 169.254.0.0
Destination/Mask   Nexthop    Flag    TimeStamp  Interface
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
```

display fib ip-prefix

Syntax

display fib ip-prefix *listname*

View

Any view

Parameter

listname Enter prefix list name, a string of one to 19 characters.

Description

Use the **display fib ip-prefix** command to view the FIB entries matching the specific prefix list.

Example

To display the FIB entries matching prefix list abc0, enter the following:

```
<4500>display fib ip-prefix abc0
Route Entry matched by prefix-list abc0:
Summary count: 3
Destination/Mask     Nexthop    Flag  TimeStamp  Interface
127.0.0.0/8          127.0.0.1  U     t[0]       InLoopBack0
127.0.0.1/32         127.0.0.1  U     t[0]       InLoopBack0
169.0.0.0/8          2.1.1.1    SU    t[0]       Vlan-interface1
```

display fib statistics

Syntax

display fib statistics [| **{ begin** | **include** | **exclude }** ***text*** **]**

View

Any view

Parameter

begin: Display the FIB entries from the first one containing the character string ***text***.

include: Display only those FIB entries containing the character string ***text***.

exclude: Display only those FIB entries excluding the character string ***text***.

text: String of specific characters.

Description

Use the **display fib statistics** command to view the total number of FIB entries.

Example

To display the total number of FIB entries, enter the following:

```
<4500>display fib statistics
Route Entry Count : 30
```

display icmp statistics

Syntax

display icmp statistics

View

Any view

Parameter

none

Description

Use the **display icmp statistics** command to view the statistics information about ICMP packets.

Related commands: **display ip interface vlan-interface**, **reset ip statistics**.

Example

To view statistics about ICMP packets, enter the following:

```
<4500> 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 13 Output Description of the **display icmp statistics** Command

Field	Description
bad formats	Number of input packets in bad format
bad checksum	Number of input packets with wrong checksum
echo	Number of input/output echo request packets
destination unreachable	Number of input/output packets with unreachable destination
source quench	Number of input/output source quench packets
redirects	Number of input/output redirected packets
echo reply	Number of input/output echo reply packets
parameter problem	Number of input/output packets with parameter problem
timestamp	Number of input/output timestamp packets
information request	Number of input information request packets
mask requests	Number of input/output mask request packets
mask replies	Number of input/output mask reply packets
information reply	Number of output information reply packets
time exceeded	Number of time exceeded packets

display ip socket

Syntax

display ip socket [socktype *sock-type*] [*task-id socket-id*]

View

Any view

Parameters

sock-type Enter the type of a socket: (tcp:1, udp 2, raw ip 3).

task-id Enter the ID of a task, with the value ranging from 1 to 100.

socket-id Enter the ID of a socket, with the value ranging from 0 to 3072.

Description

Use the **display ip socket** command to display the information about the sockets in the current system.

Example

To display the information about the socket of TCP type, enter the following:

```
<4500>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 14 Output Description of the **display ip socket** Command

Field	Description
SOCK_STREAM	The socket type
Task	The ID of a task
socketid	The ID of a socket
Proto	The protocol number used by the socket
sndbuf	The sending buffer size of the socket
rcvbuf	The receiving buffer size of the socket
sb_cc	The 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	The current data size in the receiving buffer
socket option	The option of the socket
socket state	The state of the socket

display ip statistics

Syntax

display ip statistics

View

Any view

Parameter

none

Description

Use the **display ip statistics** command to view the statistics information about IP packets.

Related commands: **display ip interface**, **reset ip statistics**.

Example

To view statistics about IP packets, enter the following:

```
<4500>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 15 Output Description of the **display ip statistics** Command

Field		Description
Input:	sum	Sum of input packets
	local	Number of received packets whose destination is the local device
	bad protocol	Number of packets with wrong protocol number
	bad format	Number of packets in bad format
	bad checksum	Number of packets with wrong checksum
	bad options	Number of packets that has wrong options
Output:	forwarding	Number of forwarded packets
	local	Number of packets that are sent by the local device
	dropped	Number of dropped packets during transmission
	no route	Number of packets that cannot be routed
	compress fails	Number of packets that cannot be compressed
Fragment:	input	Number of input fragments
	output	Number of output fragments
	dropped	Number of dropped fragments
	fragmented	Number of packets that are fragmented
	couldn't fragment	Number of packets that cannot be fragmented
Reassembling:	sum	Number of packets that are reassembled
	timeouts	Number of packets that time out

display tcp statistics

Syntax

display tcp statistics

View

Any view

Parameter

none

Description

Use the **display tcp statistics** command to view the statistics information about TCP packets.

The statistics information about TCP packets are divided into two major kinds which are Received packets and Sent packets. Each kind of packet is further divided into different kinds such as window probe packets, window update packets, duplicate packets, and out-of-order packets. Some statistics information that is closely related to TCP connection, such as window probe packets, window update packets, and data packets retransmitted, is also displayed. All of this displayed information is measured in packets.

Related commands: **display tcp status**, **reset tcp statistics**.

Example

To view statistics about TCP packets, enter the following:

```
<4500>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
```

display tcp status

Syntax

display tcp status

View

Any view

Parameter

none

Description

Use the **display tcp status** command to view the TCP connection state.

Example

To display the state of all TCP connections, enter the following:

```
<4500>display tcp status
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  EstablishedOutput
```

Table 16 Output Description of the **display tcp status** Command

Field	Description
Local Add:port	Local IP address: local port
Foreign Add:port	Remote IP address; remote port
State	State of the TCP link

display udp statistics

Syntax

display udp statistics

View

Any view

Parameter

None

Description

Use the **display udp statistics** command to view UDP traffic statistic information.

For related configuration, please refer to the **reset udp statistics** command.

Example

To display the UDP traffic statistic information, enter the following:

```
<4500>display udp statistics
```

```
Received packet:
Total:0
checksum error:0
shorter than header:0, data length larger than packet:0
no socket on port:0
broadcast:0
not delivered, input socket full:0
input packets missing pcb cache:0
Sent packet:
Total:0
```

reset ip statistics

Syntax

reset ip statistics

View

User view

Parameter

none

Description

Use the **reset ip statistics** command to clear the IP statistics information.

Related commands: **display ip interface vlan-interface**, **display ip statistics**.

Example

To clear the IP statistics information, enter the following:

```
<4500>reset ip statistics
```

reset tcp statistics

Syntax

reset tcp statistics

View

User view

Parameter

none

Description

Use the **reset tcp statistics** command to clear the TCP statistics information.

Related command: **display tcp statistics**.

Example

To clear the TCP statistics information, enter the following:

```
<4500>reset tcp statistics
```

reset udp statistics

Syntax

reset udp statistics

View

User view

Parameter

None

Description

Use the **reset udp statistics** command to clear the UDP statistics information.

Example

To clear the UDP traffic statistics information, enter the following:

```
<4500>reset udp statistics
```

tcp timer fin-timeout

Syntax

tcp timer fin-timeout ***time-value***

undo tcp timer fin-timeout

View

System View

Parameter

time-value Enter the TCP finwait timer value in second, with the value ranging from 76 to 3600; By default, 675 seconds.

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.

When the TCP connection state changes from FIN_WATI_1 to FIN_WAIT_2, the finwait timer is enabled. If the switch does not receive FIN packet before finwait timer timeouts, the TCP connection will be terminated.

Related commands: **tcp timer syn-timeout**, **tcp window**.

Example

To configure the TCP finwait timer value as 800 seconds, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]tcp timer fin-timeout 800
```

tcp timer syn-timeout

Syntax

tcp timer syn-timeout ***time-value***

undo tcp timer syn-timeout

View

System View

Parameter

time-value Enter the TCP synwait timer value measured in second, whose value ranges from 2 to 600. The default time-value is 75 seconds.

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 timer.

TCP will enable the synwait timer, if a SYN packet is sent. The TCP connection will be terminated If the response packet is not received.

Related commands: **tcp timer fin-timeout**, **tcp window**.

Example

To configure the TCP synwait timer value as 80 seconds, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]tcp timer syn-timeout 80
```

tcp window

Syntax

tcp window *window-size*

undo tcp window

View

System View

Parameter

window-size Enter the size of the transmission and receiving buffers measured in kilobytes (KB), whose value ranges from 1 to 32. By default, the window-size is 4KB.

Description

Use the **tcp window** command to configure the size of the transmission and receiving buffers of the connection-oriented Socket.

Use the **undo tcp window** command to restore the default size of the buffer.

Related commands: **tcp timer fin-timeout**, **tcp timer syn-timeout**.

Example

To configure the size of the transmission and receiving buffers as 3KB, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]tcp window 3
```

6 USING ROUTING PROTOCOL COMMANDS

This chapter describes how to use the following commands:

Routing Table Display Commands

- display ip routing-table
- display ip routing-table acl
- display ip routing-table ip_address
- display ip routing-table ip_address1 ip_address2
- display ip routing-table ip-prefix
- display ip routing-table protocol
- display ip routing-table radix
- display ip routing-table statistics
- display ip routing-table verbose

Static Route Configuration Command

- delete static-routes all
- ip route-static

RIP Configuration Commands

- checkzero
- default cost
- display rip
- filter-policy export
- filter-policy import
- host-route
- import-route
- network
- peer
- preference
- reset
- rip
- rip authentication-mode
- rip input

Routing Table Display Commands

This section describes the commands you can use to display routing table information.

When the Switch 4500 runs a routing protocol, it is able to perform the functions of a router. The term router in this section can refer either to a physical router, or to the Switch 4500 running a routing protocol.

display ip routing-table

Syntax

```
display ip routing-table
```

View

All views

Parameter

None

Description

Use the **display ip routing-table** command to view a summary of routing table information

Each line in the table represents one route. The displayed information includes destination address/mask length, protocol, preference, cost, next hop and output interface.

Only the currently used route, that is the best route, is displayed.

Example

To view a summary of routing table information, enter the following:

```
<4500>display ip routing-table
```

The information displays in the following format:

```
Routing Table: public net
Destination/Mask Proto   Pre Cost      Nexthop         Interface
1.1.1.0/24       DIRECT  0   0         1.1.1.1         Vlan-interface1
1.1.1.1/32       DIRECT  0   0         127.0.0.1       InLoopBack0
2.2.2.0/24       DIRECT  0   0         2.2.2.1         Vlan-interface2
2.2.2.1/32       DIRECT  0   0         127.0.0.1       InLoopBack0
3.3.3.0/24       DIRECT  0   0          3.3.3.1        Vlan-interface3
3.3.3.1/32       DIRECT  0   0         127.0.0.1       InLoopBack0
4.4.4.0/24       DIRECT  0   0         4.4.4.1         Vlan-interface4
4.4.4.1/32       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
```

Table 17 Output Description of the **display ip routing-table** Command

Field	Description
Destination/Mask	Destination address/Mask length
Protocol	Routing protocol
Pre	Routing preference
Cost	Cost
Interface	Output interface, through which the data packet destined for the destination network is sent

display ip routing-table acl

Syntax

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

View

All views.

Parameters

acl_number Enter the number of the IP ACL, in the range 2000 to 2999.

verbose Enter to display verbose information about both the active and inactive routes that passed filtering rules. If you do not enter this parameter, the command only displays a summary of the active routes that passed filtering rules.

Description

Use the **display ip routing-table acl** command to view the route filtered through the specified ACL.

This command is used to display the routes that passed the filtering rules in the specified ACL.

The command only displays routes that passed basic ACL filtering rules.

Example

To display a summary of the active routes filtered through basic ACL 2000, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]acl number 2000
[4500-acl-basic-2000]rule permit source 10.1.1.1 0.0.0.255
[4500-acl-basic-2000]rule deny source any
[4500-acl-basic-2000]display ip routing-table acl 2000
```

The information displays in the following format:

```
Routes matched by access-list 2000:
Summary count: 42
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
```

For detailed description of the output information, see Table 18.

To display the verbose information of the active and inactive routes that are filtered through basic ACL 2000.

```
<4500>display ip routing-table acl 2000 verbose
```

The information displays in the following format:

```
Routes matched by access-list 2000:
Generate Default: no
+ = 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)
   Vlinkindex: 0
   State:  <Int ActiveU Retain Unicast>
   Age: 7:24  Cost: 0/0  Tag: 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)
Vlinkindex: 0
State: <NoAdvise Int ActiveU Retain Gateway Unicast>
   Age: 7:24  Cost: 0/0  Tag: 0
```

Table 18 Output Description of the **ip routing-table acl verbose** Command

Field	Description
Destination	Destination address
Mask	Mask
Protocol	Routing protocol
Preference	Routing preference
Nexthop	Next hop address

Table 18 Output Description of the **ip routing-table acl verbose** Command

Field	Description
Interface	Output interface, through which the data packet destined for the destination network is sent
Vlinkindex	Virtual link index
State	Route state description:
	ActiveU — The route is selected and is optimum
	Blackhole — Blackhole route is similar to Reject route, but it will not send the ICMP unreachable message to the source end
	Delete — The route is deleted
	Gateway — Identifies that the route is not an interface route
	Hidden — The route exists, but it is unavailable temporarily for some reasons (e.g., configured policy or interface is Down). Moreover, you do not wish to delete it. Therefore, you need to hide it, so as to restore it again later
	Holddown — Holddown is one kind of route redistribution policy adopted by some distance-vector (D-V) routing protocols (e.g., RIP), through which these routing protocols can avoid the flooding of error routes and deliver the routing unreachable message accurately. For example, the RIP redistributes a certain route every a period of time regardless of whether the actually found routes destined for the same destination change. For more details, refer to the specific routing protocols
	Int — The route is discovered by interior gateway protocol (IGP)
	NoAdvise — The routing protocol does not redistribute NoAdvise route when it redistributes routes based on the policy
	NotInstall — The routing protocol generally selects the route with the highest precedence from its routing table, then places it in its core routing table and redistributes it. Although the NotInstall route cannot be placed in the core routing table, it is possibly that it is selected and redistributed
	Reject — Unlike the normal routes, the Reject route will discard the packets that select it as their route, and the router will send ICMP unreachable message to the source end. Reject route is usually used for the network test
	Retain — When the routes from the routing table are deleted, the routes with Retain flag will not be deleted. Using this function you can set Retain flag for some static routes, so that they can exist in the core routing table
	Static — The route with Static flag will not be cleared from the routing table after you save it and reboot the router. Generally, the static route configured manually in the router belongs to a Static route
	Unicast — Unicast route
Age	Time to live
Cost	Value of cost
Tag	Tag of the route

display ip routing-table ip_address

Syntax

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

View

All views

Parameters

ip_address Enter the destination IP address.

mask Enter either the IP subnet mask (in x.x.x.x format), or the subnet mask length (in the range 0 to 32). Optional.

longer-match Enter to display an address route that matches the destination IP address in natural mask range. Optional.

verbose Enter to display verbose information about both active and inactive routes. Without this parameter, this command only displays a summary of active routes. Optional.

Description

Use the **display ip routing-table** ip_address command to view routing information for a specific IP address, and you can also choose the type of information to display. If the destination address, ***ip_address***, has a corresponding route in natural mask range, this command will display all subnet routes or only the route best matching the destination address, ***ip_address***, is displayed. And only the active matching route is displayed.

Use the **display ip routing-table *ip_address mask*** command to display the route that matches the specified IP destination address and subnet mask.

Use the **display ip routing-table *ip_address* longer-match** command to display all destination address routes that match destination IP addresses in natural mask range.

Use the **display ip routing-table *ip_address* verbose** command to display verbose information about both active and inactive routes.

Example

There is corresponding route in natural mask range. Display the summary.

```
<4500>display ip routing-table 169.0.0.0
Destination/Mask   Proto   Pre     Cost Nexthop    Interface
169.0.0.0/16       Static  60      0    2.1.1.1    LoopBack1
```

There are corresponding routes in the natural mask range. Display the detailed information.

```
<4500>display ip routing-table 169.0.0.0 verbose
Routing tables:
+ = Active Route, - = Last Active, # = Both* = Next hop in use
Summary count:2
**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)
   Vlinkindex: 0
   State: <Int ActiveU Gateway Static Unicast>
   Age: 3:47    Cost: 0/0
**Destination: 169.0.0.0   Mask: 255.254.0.0
```

```
Protocol: #Static        Preference: 60
*NextHop: 2.1.1.1        Interface: 2.1.1.1(LoopBack1)
Vlinkindex: 0
State: <Int ActiveU Static Unicast>
Age: 4:479    Cost: 0/0  Tag: 0
```

For detailed description of output information, refer to Table 18.

display ip routing-table ip_address1 ip_address2

Syntax

display ip routing-table *ip_address1 mask1 ip_address2 mask2*
[verbose]

View

All views

Parameters

ip_address1 mask1 Enter the destination IP address and subnet mask that you want to start the address range. This command displays the route for your chosen address range. The subnet mask can be entered as either a dotted decimal notation (x.x.x.x), or an an integer in the range 0 to 32.

ip_address2 mask2 Enter the IP address and subnet mask that you want to end the address range. The subnet mask can be entered as either a dotted decimal notation (x.x.x.x), or an integer in the range 0 to 32.

verbose Enter to display the verbose information of both the active and inactive routes. Without this parameter, the command only displays a summary of active routes. Optional.

Description

Use the **display ip routing-table *ip_address1 mask1 ip_address2 mask2*** command to view the route information for the specified address range.

Example

To display the routing information of destination addresses ranging from 1.1.1.0 to 2.2.2.0., with a subnet mask of 24, enter the following:

```
<4500>display ip routing-table 1.1.1.0 24 2.2.2.0 24
```

The information displays in the following format:

```
Routing tables:
  Summary count: 3
Destination/Mask    Proto   Pre Cost Nexthop   Interface
1.1.1.0/24          DIRECT  00       1.1.1.1   Vlan-interface1
1.1.1.1/32          DIRECT  00       127.0.0.1 InLoopBack0
2.2.2.0/24          DIRECT  00       2.2.2.1   Vlan-interface2
```

For a detailed description of the output information, refer to Table 17.

display ip routing-table ip-prefix

Syntax

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

View

All views

Parameter

ip_prefix_name Enter the ip prefix list name.

verbose Enter to display verbose information about both the active and inactive routes that passed filtering rules. Without this parameter, this command displays the summary of active routes that passed filtering rules.

Description

Use the command **display ip routing-table ip-prefix** to view information on the routes that passed filtering rules for the specified IP prefix name.

Example

To display the summary information for ip prefix list abc2, active route only, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]ip ip-prefix abc2 permit 10.1.1.0 24 less-equal 32
[4500]display ip routing-table ip-prefix abc2
```

The information displays in the following format:

```
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
```

For a detailed description of the output information, see Table 18.

To display the information on the active and inactive routes for prefix list abc2, enter the following:

```
[4500]display ip routing-table ip-prefix abc2 verbose
```

The information displays in the following format:

```
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)
   Vlinkindex: 0
   State:  <Int ActiveU Retain Unicast>
   Age: 3:23:44    Cost: 0/0    Tag: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)
   Vlinkindex: 0
State: <NoAdvise Int ActiveU Retain Gateway Unicast>
   Age: 3:23:44    Cost: 0/0    Tag: 0
```

For detailed information of the output information, refer to Table 18.

display ip routing-table protocol

Syntax

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

View

All views

Parameters

protocol Enter one of the following:

- **direct** Displays the direct connection route information
- **static** Displays the static route information.
- **ospf** Displays OSPF route information.
- **ospf-ase** Displays OSPF ASE route information.
- **ospf-nssa** Displays OSPF NSSA route information.
- **rip** Displays RIP route information.

inactive Enter to display inactive route information. Without this parameter, the command displays both active and inactive route information. Optional.

verbose Enter to display verbose route information. Without this parameter, the command displays the route summary. Optional.

Description

Use the **display ip routing-table protocol** command to view the route information for a specified protocol.

Example

To display a summary of all direct connection routes, enter the following:

```
<4500>display ip routing-table protocol direct
```

The information displays in the following format:

```
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
```

To display a summary of all static route information, enter the following:

```
<4500>display ip routing-table protocol static
```

The information displays in the following format:

```
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-interface2
```

The displayed information helps you to confirm whether the configuration of the static routing is correct.

For detailed description of the output, refer to Table 17.

display ip routing-table radix

Syntax

display ip routing-table radix

View

All views

Parameter

None

Description

Use the **display ip routing-table radix** command to view the route information in a tree structure.

Example

To display the route information, enter the following:

```
<4500>display ip routing-table radix
```

The information displays in the following format:

```
Radix tree for INET (2) inodes 7 routes 5:
          +-32+--{210.0.0.1
        +--0+
         | | +--8+--{127.0.0.0
         | | | +-32+--{127.0.0.1
         | +--1+
         | +--8+--{20.0.0.0
         | +-32+--{20.1.1.1
```

Table 19 Output Description of the **display ip routing-table radix** Command

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

display ip routing-table statistics

Syntax

display ip routing-table statistics

View

All views

Parameter

None

Description

Use the **display ip routing-table statistics** command to display the routing information for all protocols.

The information includes the number of routes per protocol, the number of active routes per protocol, the number of routes added and deleted per protocol, and the number of routes that are labeled deleted but that are not deleted per protocol. The total number of routes in each of these categories is also displayed.

Example

To display the integrated route information, enter the following:

```
<4500>display ip routing-table statistics

Routing tables:
Proto      route       active      added       deleted
DIRECT     2           2           2           0
STATIC     0           0           0           0
RIP        0           0           0           0
TOTAL      2           2           2           0
```

Table 20 Output Description of the **display ip routing-table statistics** Command

Field	Description
Proto	Routing protocol
route	Number of routes
active	Number of active routes
added	Number of added routes after the router is rebooted or the routing table is cleared last time.
deleted	Number of deleted routes (such routes will be freed in a period of time)

display ip routing-table verbose

Syntax

display ip routing-table verbose

View

All views

Parameter

None

Description

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

The information displayed includes the route state, the verbose description of each route and the statistics of the entire routing table.

All current routes, including inactive routes and invalid routes, are displayed.

Example

To display the verbose routing table information, enter the following:

```
<4500>display ip routing-table verbose
```

The information displays in the following format:

```
Routing Tables:
  + = Active Route, - = Last Active, # = Both    * = Next hop in use
  Destinations: 3       Routes: 3
  Holddown: 0    Delete: 62      Hidden: 0
**Destination: 1.1.1.0           Mask: 255.255.255.0
         Protocol: #DIRECT       Preference: 0
         *NextHop: 1.1.1.1          Interface:
1.1.1.1(Vlan-interface1)
         State: <Int ActiveU Retain Unicast>
         Age: 20:17:41   Cost: 0/0
**Destination: 1.1.1.1           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: 20:17:42   Cost: 0/0
**Destination: 2.2.2.0           Mask: 255.255.255.0
         Protocol: #DIRECT       Preference: 0
         *NextHop: 2.2.2.1          Interface:
2.2.2.1(Vlan-interface2)
         State: <Int ActiveU Retain Unicast>
         Age: 20:08:05   Cost: 0/0
```

The meaning of route state is defined in Table 18. Other generated information is described in Table 21.

Table 21 Output Description of the **display ip routing-table verbose** Command

Descriptor	Meaning
Holddown	The number of holddown routes. This refers to a route advertising policy that some distance vector routing protocols (such as RIP) use to avoid expansion of error routes and to improve the transmission speed and accuracy of unreachable routes. It usually advertises a static route at an interval, regardless of the changes to dynamic routes to the same destination. For details, see the specific routing protocol.
Delete	The number of deleted routes.
Hidden	The number of hidden routes, that is routes not available at present but still required. They can be hidden for future use.

Static Route Configuration Command

This section describes the command you can use to configure a static route.

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 the static routes.

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

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

Example

Delete all the static routes in the router.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]delete static-routes all
Are you sure to delete all the unicast static routes?[Y/N]
```

ip route-static

Syntax

ip route-static *ip_address* { *mask* | *mask-length* } { *interface_name* | *gateway_address* } [preference *preference_value*] [reject | blackhole]

undo ip route-static *ip_address* { *mask* | *mask_length* } [*interface_name* | *gateway_address*] [preference *preference_value*] [reject | blackhole]

View

System view

Parameters

ip_address Enter the destination IP address in dotted decimal notation.

mask Enter the IP subnet mask.

mask-length Enter the number of consecutive 1s in the mask. Because 1s in the 32-bit mask must be consecutive, the mask in dotted decimal format can be replaced by ***mask-length***.

interface_name Specify the transmission interface name of the route. Packets that are sent to a NULL interface, are discarded immediately which decreases the system load.

gateway_address Specify the next hop IP address of the route.

preference_value Enter the preference level of the route in the range 1 to 255. The default preference is 60.

reject Enter to indicate an unreachable route.

blackhole Enter to indicate a blackhole route.

Description

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

Use the **undo ip route-static** command to delete the configured static route.

By default, the system can access the subnet route directly connected to the router. If you do not use the parameters **preference**, **reject** or **blackhole**, the route will be reachable by default with a preference level of 60.

A static route is a special route. You can set up an interconnecting network with a static route configuration. The problem for such configuration is when a fault occurs to the network, the static route cannot change automatically to steer away from the node causing the fault without the help of an administrator.

In a relatively simple network, a system administrator may chose to implement static routes rather than a dynamic routing protocol. The proper configuration and usage of static routes can improve the network performance and ensure bandwidth for important applications.

All the following routes are static routes:

- Reachable route — A normal route. That is, the IP packet is sent to the next hop via the route marked by the destination. It is the most common type of static route.
- Unreachable route — When a static route to a destination has the "reject" attribute, all the IP packets to this destination will be discarded, and the originating host will be informed destination unreachable.
- Blackhole route — If a static route to a destination has the "blackhole" attribute, the outgoing interface of this route is the Null 0 interface regardless of the next hop address, and all the IP packets addressed to this destination are dropped without notifying the source host.

The attributes **reject** and **blackhole** are usually used to control the range of reachable destinations of this router and to help troubleshoot the network.

Use the following precautions when configuring a static route:

- You cannot specify an interface address of the local Switch as the next hop address of a static route.
- When the destination IP address and subnet mask are both set to 0.0.0.0, this is the configured default route. A packet is forwarded using the default route as a last resort if no better routing match is found in the routing table.
- As an alternative way to configure preference level, a flexible routing protocol can be adopted.

Related command: **display ip routing-table**, **delete static-routes all**.

Example

To configure the next hop of the default route as 129.102.0.2, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]ip route-static 0.0.0.0 0.0.0.0 129.102.0.2
```

RIP Configuration Commands

This section describes the commands you can use to configure the Routing Information Protocol (RIP).

When the Switch 4500 runs a routing protocol, it is able to perform the functions of a router. The term router in this section can refer either to a physical router or to the Switch 4500 running a routing protocol.

checkzero

Syntax

checkzero

undo checkzero

View

RIP view

Parameter

None

Description

Use the **checkzero** command to check the zero field of RIP-1 packets. By default, RIP-1 performs zero field checking.

Use the **undo checkzero** command to disable the checking of the zero fields.

According to the RFC1058 protocol specifications, some fields in RIP-1 packets must be set to zero. These are called zero fields. During the zero check operation, if a RIP-1 packet is received in which the zero fields are not zeros, it will be rejected. Use the **checkzero** command to enable or disable the zero check operation on RIP-1.

This command does not work with RIP-2 packets, since RIP-2 packets have no zero fields.

Example

To configure the Switch not to perform zero checking for RIP-1 packet, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]rip
[4500-rip]undo checkzero
```

default cost

Syntax

default cost *value*

undo default cost

View

RIP view

Parameter

value Enter the default routing cost, in the range 1 to 16. The default is 1.

Description

Use the **default cost** command to set the default routing cost of an imported route.

Use the **undo default cost** command to restore the default value.

If you do not specify a routing cost when using the **import-route** command, the default cost you specify here is used.

Related command: **import-route**.

Example

To set the default routing cost of the imported route of another routing protocol to 3, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]rip
[4500-rip]default cost 3
```

display rip

Syntax

display rip

View

All views

Parameter

None

Description

Use the **display rip** command to view the current RIP running state and its configuration information.

Example

To display the current running state and configuration information of RIP, enter the following:

```
<4500>display rip
RIP is running
  public net VPN-Instance
    Checkzero is on         Default cost : 1
    Summary is on          Preference : 100
    Period update timer : 30
    Timeout timer : 180
```

```
Garbage-collection timer : 120
No peer router
Network :
202.38.168.0
```

Table 22 Output Description of the **display rip** Command

Field	Description
RIP is running	RIP is active
Checkzero is on	Zero field checking is enabled
Default cost:1	The default route cost is 1
Summary is on	Routes are summarized automatically
Preference: 100	The preference of RIP is 100
Period update timer : 30	The three RIP timers
Timeout timer : 180	
Garbage-collection timer : 120	
No peer router	No destination address of a transmission is specified
Network: 202.38.168.0	RIP enabled on network segment 202.38.168.0

filter-policy export

Syntax

filter-policy { *acl_number* | gateway *gateway-ip* | ip-prefix *ip_prefix_name* } export [*routing_process*]

filter-policy route-policy *route-policy-name* export

undo filter-policy { *acl_number* | gateway *gateway-ip* | ip-prefix *ip_prefix-name* } export [*routing_process*]

undo filter-policy route-policy *route-policy-name* export

View

RIP view

Parameters

acl_number Enter the number of the ACL that you want to use to filter the destination addresses of the routing information.

gateway-ip

ip_prefix_name Enter the name of the address prefix list that you want to use to filter the destination addresses of the routing information.

route-policy-name: Route policy name that filters routing information. After enabling RIP protocol, you can determine which routes are to be sent/received based on acl/cost/interface/ip/ip-prefix/tag fields.

routing_protocol Enter the routing protocol whose routing information is to be filtered. This can be one of the following:

- **direct** — Specifies direct routes
- **static** — Specifies static routes.

Description

Use the **filter-policy export** command to configure RIP to filter the advertised routing information.

Use the **undo filter-policy export** command to configure RIP not to filter the advertised routing information. This is the default.

Related commands: **acl**, **filter-policy import**, **ip ip-prefix**.

Example

To filter the advertised route information using ACL 2000, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]rip
[4500-rip]filter-policy 2000 export
```

filter-policy import

Syntax

filter-policy gateway ***ip_prefix_name*** **import**

undo filter-policy gateway ***ip_prefix_name*** **import**

filter-policy { ***acl_number*** | **ip-prefix** ***ip_prefix_name*** **[gateway** ***ip_prefix_name*** **]** | **route-policy** ***route-policy-name*** } **import**

undo filter-policy { ***acl_number*** | **ip-prefix** ***ip_prefix_name*** | **[gateway** ***ip_prefix_name*** **]** | **route-policy** ***route-policy-name*** } **import**

View

RIP View

Parameters

gateway ***ip_prefix_name*** Enter the name of the address prefix list. This is used to filter the addresses of the neighboring routers that are advertising the routing information.

acl_number Enter an ACL number. This is used to filter the destination addresses of the routing information.

ip_prefix_name Enter the name of the address prefix list. This is used to filter the destination addresses of the routing information.

route-policy-name: Route policy name that filters routing information. After enabling RIP protocol, you can determine which routes are to be sent/received based on acl/cost/interface/ip/ip-prefix fields.

Description

Use the **filter-policy gateway import** command to configure the switch to filter the routing information received from a specified address.

Use the **undo filter-policy gateway import** command to configure the switch not to filter the routing information received from the specified address.

Use the **filter-policy import** command to configure the switch to filter global routing information.

Use the **undo filter-policy import** command to disable filtering of received global routing information.

By default, RIP does not filter the received routing information.

Related commands: **acl, filter-policy export, ip ip-prefix.**

Example

To configure the filtering of the global routing information using acl 2000, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]rip
[4500-rip]filter-policy 2000 import
```

host-route

Syntax

host-route

undo host-route

View

RIP view

Parameter

None

Description

Use the **host-route** command to configure RIP to accept host routes. This is the default.

Use the **undo host-route** command to configure RIP to reject host routes.

Example

To configure RIP to reject a host route, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]rip
[4500-rip]undo host-route
```

import-route

Syntax

import-route ***protocol*** **[cost** ***value*** | **route-policy** ***route-policy-name*** **]**

undo import-route ***protocol***

View

RIP view

Parameters

protocol Enter the routing protocol to be imported. This can be one of the following: **direct** or **static**.

value Enter the cost value of the route to be imported.

route-policy ***route_policy_name*** Enter a route-policy name. Only routes that match the conditions of the specified policy are imported.

Description

Use the **import-route** command to import the routes of other protocols into RIP.

Use the **undo import-route** command to cancel the import of routes from other protocols. By default, RIP does not import any other protocol's route.

The **import-route** command can be used to import the route of another protocol with a certain cost value. RIP regards the imported route as its own route and transmits it with the specified cost value. This command can greatly enhance the RIP capability of obtaining routes, thus increases the RIP performance.

If the **cost** ***value*** is not specified, routes will be imported according to the **default cost** ranging from 1 to 16. If the imported route cost value is 16, then RIP continues to announce this cost to other routers running RIP, and marks this route with HOLDDOWN. However, this router can still forward packets until the Garbage Collection timer times out (defaults to 120 seconds).

Related commands: **default cost**.

Example

To import a static route with a cost of 4, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]rip
[4500-rip]import-route static cost 4
```

network

Syntax

network ***network_address***

undo network ***network_address***

View

RIP view

Parameter

network_address Enter the IP network address of an interface.

Description

Use the **network** command to enable Routing Information Protocol (RIP) on the interface of a specified network segment connected to the router.

Use the **undo network** command to disable RIP on the interface. By default, RIP is disabled on an interface.

After you have enabled RIP, you must also enable RIP for a specified interface using this command. RIP only operates on the interface of specified network segments.

The **undo network** command is similar to the **undo rip work** command in the VLAN Interface View, in that an interface using either command will result in the interface not receiving/transmitting RIP routes. However, if you use **undo rip work**, other interfaces will still forward the routes of the interfaces set to **undo rip work**. If you use **undo network**, other interfaces will not forward the routes of interfaces set to **undo network**.

When the **network** command is used on an IP address, the interface on this network segment is enabled. For example, if you view the **network** 129.102.1.1 with both the **display current-configuration** command and the **display rip**, the IP address is shown as 129.102.0.0.

Related commands: **rip work**.

Example

To enable RIP on the interface with the network address 129.102.0.1, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]rip
[4500-rip]network 129.102.0.0
```

peer

Syntax

peer ***ip_address***

undo peer ***ip_address***

View

RIP view

Parameter

ip_address Enter the interface IP address of the peer router.

Description

Use the peer command to configure the destination address of the peer device.

Use the **undo peer** command to cancel the set destination address. By default, there is no destination address.

3Com recommends that you do not use this command. RIP can use unicast to exchange information with non-broadcasting networks. If required, you can use this command to specify the destination address of the peer device.

Example

To specify the sending destination address as 202.38.165.1, enter the following:

```
<4500>system-view
```

```
System View: return to User View with Ctrl+Z.
[4500]rip
[4500-rip]peer 202.38.165.1
```

preference

Syntax

preference *value*

undo preference

View

RIP view

Parameter

value Enter the preference level, in the range 1 to 255. By default, the value is 100.

Description

Use the **preference** command to configure the route preference of RIP.

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

The default value of each routing protocol is determined by the specific routing policy. This "preference" determines the optimal route in the IP routing table. You can use this command to modify the RIP preference.

Example

To specify a RIP preference of 20, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]rip
[4500-rip]preference 20
```

reset

Syntax

reset

View

RIP view

Parameter

None

Description

Use the **reset** command to reset the system configuration parameters of RIP.

When you need to re-configure parameters of RIP, this command can be used to restore to the default setting.

Example

Reset the RIP system.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
```

```
[4500]rip
[4500-rip]reset
```

rip

Syntax

rip

undo rip

View

System view

Parameter

None

Description

Use the **rip** command to enable RIP and enter the RIP command view. From here, you can configure RIP using the other commands described in this section.

Use the **undo rip** command to disable RIP. By default, RIP is disabled.

Enabling RIP does not affect interface configurations.

Example

To enable RIP, and enter RIP view, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]rip
[4500-rip]
```

rip authentication-mode

Syntax

rip authentication-mode { simple *password* | md5 { usual *key-string* | nonstandard *key-string key-id* }}

undo rip authentication-mode

View

Interface View

Parameters

simple Enter to specify simple text authentication mode.

password Enter the simple text authentication key.

md5 Enter to specify MD5 cipher text authentication mode.

usual Enter to specify the MD5 cipher text authentication packet to use the general packet format (RFC1723 standard format).

key-string Enter the MD5 cipher text authentication key. If it is entered in plain text, the MD5 key is a character string not exceeding 16 characters. This key is displayed in a cipher text form in a length of 24 characters when **display**

current-configuration command is executed. Inputting the MD5 key in cipher text form with 24 characters long is also supported.

nonstandard: Enter to set the MD5 cipher text authentication packet to use a packet format (as described in RFC2082).

key-id Enter an MD5 cipher text authentication identifier, ranging from 1 to 255.

Description

Use the **rip authentication-mode** command to configure the RIP-2 authentication mode and its parameters for the Switch 4500.

Use the **rip authentication-mode simple** command to configure the RIP-2 simple text authentication key.

Use the **rip authentication-mode md5 usual *key-string*** to configure the MD5 cipher text authentication key for RIP-2.

Use the **rip authentication-mode md5 nonstandard *key-string* *key-id*** command to configure the MD5 cipher text authentication ID for RIP-2.

Use the **undo rip authentication-mode** command to cancel RIP-2 authentication.

There are two RIP-2 authentication modes: simple authentication and MD5 cipher text authentication. When you use MD5 cipher text authentication mode, two types of packet formats are available. The standard format (set using the **usual** parameter), is described in RFC 1723. The non-standard format (set using the **nonstandard** parameter), is described in RFC 2082.

RIP-1 does not support authentication.

Related command: **rip version**.

Example

To specify the interface "Vlan-interface 1" to use **simple** authentication with the key set to "aaa", enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface Vlan-interface 1
[4500-Vlan-interface1]rip version 2
[4500-Vlan-interface1]rip authentication-mode simple aaa
[4500-Vlan-interface1]quit
```

To specify the interface Vlan-interface 1 to use MD5 authentication with the key string as "aaa" and the packet type set to **usual**, enter the following:

```
[4500]interface Vlan-interface 1
[4500-Vlan-interface1]rip version 2
[4500-Vlan-interface1]rip authentication-mode md5 key-string aaa
[4500-Vlan-interface1]rip authentication-mode md5 type nonstandard
```

To set MD5 authentication on Vlan-interface 1 with the key string set to "aaa" and the packet type set to **usual**, enter the following:

```
[4500]interface Vlan-interface 1
[4500-Vlan-interface1]rip version 2
[4500-Vlan-interface1]rip authentication-mode md5 usual aaa
```

rip input

Syntax

rip input

undo rip input

View

Interface View

Parameter

None

Description

Use the **rip input** command to allow an interface to receive RIP packets. By default, all interfaces except loopback interfaces are able to receive RIP packets.

Use the **undo rip input** command to block an interface from receiving RIP packets.

This command is used in conjunction with two other two commands: **rip output** and **rip work**. The **rip input** and **rip output** commands control, respectively, the receipt and the transmission of RIP packets on an interface. The **rip work** command allows both receipt and transmission of RIP packets.

Related commands: **rip output**, **rip work**.

Example

To set the interface Vlan-interface 1 not to receive RIP packets, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface Vlan-interface 1
[4500-Vlan-interface1]undo rip input
```

rip metricin

Syntax

rip metricin ***value***

undo rip metricin

View

Interface View

Parameter

value Enter an additional route metric to be added when receiving a packet, ranging from 0 to 16. By default, the value is 0.

Description

Use the **rip metricin** command to configure an additional route metric to be added to the route when an interface receives RIP packets.

Use the **undo rip metricin** command to restore the default value of this additional route metric.

Related command: **rip metricout**.

Example

To set the additional route metric to 2 when the interface Vlan-interface 1 receives RIP packets, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface Vlan-interface 1
[4500-Vlan-interface1]rip metricin 2
```

rip metricout

Syntax

rip metricout ***value***

undo rip metricout

View

Interface View

Parameter

value Enter an additional route metric added when transmitting a packet, ranging from 1 to 16. By default, the value is 1.

Description

Use the **rip metricout** command to configure an additional route metric to be added to a route when an interface transmits RIP packets.

Use the **undo rip metricout** command to restore the default value of the additional route metric.

Related command: **rip metricin**.

Example

To set the additional route metric to 2 when the interface Vlan-interface 1 transmits RIP packets, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface Vlan-interface 1
[4500-Vlan-interface1]rip metricout 2
```

rip output

Syntax

rip output

undo rip output

View

Interface View

Parameter

None

Description

Use the **rip output** command to allow an interface to transmit RIP packets.

Use the **undo rip output** command to disable an interface from transmitting RIP packets.

By default, all interfaces except loopback interfaces are able to transmit RIP packets.

This command is used in conjunction with two other commands: **rip input** and **rip work**. **rip input** and **rip output** control, respectively, the receipt and the transmission of RIP packets on an interface. **rip work** allows both receipt and transmission of RIP packets.

Related commands; **rip input**, **rip work**.

Example

To prevent the interface Vlan-interface 1 from transmitting RIP packets, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface Vlan-interface 1
[4500-Vlan-interface1]undo rip output
```

rip split-horizon

Syntax

rip split-horizon
undo rip split-horizon

View

Interface View

Parameter

None

Description

Use the **rip split-horizon** command to configure an interface to use split horizon when transmitting RIP packets. This is the default.

Use the **undo rip split-horizon** command to configure an interface not to use split horizon when transmitting RIP packets.

Normally, split horizon is necessary for preventing router loops. You may need to disable split horizon to ensure proper operation of protocols.

Example

To set the interface Vlan-interface 1 not to use split horizon when processing RIP packets, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface Vlan-interface 1
[4500-Vlan-interface1]undo rip split-horizon
```

rip version

Syntax

```
rip version 1
rip version 2 [ broadcast | multicast ]
undo rip version
```

View

Interface View

Parameters

1 Enter to set the interface version to RIP-1.

2 Enter to set the interface version to RIP-2.

broadcast Enter to set the transmission mode of a RIP-2 packet to broadcast.

multicast Enter to set the transmission mode of a RIP-2 packet to multicast.

Description

Use the **rip version** command to configure the version number of RIP packets on an interface.

Use the **undo rip version** command to restore the default RIP packet version on the interface. The interface RIP version is RIP-1.

By default, RIP-1 transmits packets in broadcast mode, while RIP-2 transmits packets in multicast mode.

When running RIP-1, the interface receives and transmits RIP-1 packets, and can also receive RIP-2 broadcast packets.

When running RIP-2 in broadcast mode, the interface receives and transmits RIP-2 broadcast packets, and can also receive both RIP-1 packets and RIP-2 multicast packets.

When running RIP-2 in multicast mode, the interface receives and transmits RIP-2 multicast packets, and can also receive RIP-2 broadcast packets. The interface can not receive RIP-1 packets.

Example

To configure the interface Vlan-interface 1 to RIP-2 broadcast mode, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface Vlan-interface 1
```

```
[4500-Vlan-interface1]rip version 2 broadcast
```

rip work

Syntax

rip work

undo rip work

View

Interface View

Parameter

None

Description

Use the **rip work** command to enable the RIP on an interface. This is the default.

Use the **undo rip work** command to disable RIP on an interface.

This command is used in conjunction with the **rip input**, **rip output** and **network** commands. Refer to the descriptions of these commands for details.

Related commands: **network**, **rip input**, **rip output**.

Example

To disable the running of RIP on interface Vlan-interface 1, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface Vlan-interface 1
[4500-Vlan-interface1]undo rip work
```

summary

Syntax

summary

undo summary

View

RIP view

Parameter

None

Description

Use the **summary** command to activate RIP-2 automatic route summarization. This is the default.

Use the **undo summary** command to disable RIP-2 automatic route summarization.

Route aggregation can be performed to reduce the routing traffic on the network as well as to reduce the size of the routing table. RIP-1 does not support subnet masks. Forwarding subnetted routes may cause ambiguity. Networks that use RIP-1 should always use the natural mask. Therefore, RIP-1 uses route

summarization all the time. If RIP-2 is used, route summarization function can be disabled with the **undo summary** command, when it is necessary to broadcast the subnet route.

Related command: **rip version**

Example

To set the RIP version on the interface Vlan-interface 1 to RIP-2, and then disable the route aggregation, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface Vlan-interface 1
[4500-Vlan-interface1]rip version 2
[4500-Vlan-interface1]quit
[4500]rip
[4500-rip]undo summary
```

timers

Syntax

timers { update ***update-timer-length*** **| timeout** ***timeout-timer-length*** **} ***

undo timers { update | timeout } *

View

RIP View

Parameters

update-timer-length Enter the value of the period update timer, ranging from 1 to 3600 seconds. The default value is 30 seconds.

timeout-timer-length Enter the value of the timeout timer, ranging from 1 to 3600 seconds. The default value is 180 seconds.

Description

Use the **timers** command to modify the values of the three RIP timers: period update, timeout, and garbage-collection.

Use the **undo timers** command to restore the default settings.

By default, the values of period update, timeout, and garbage-collection timers are 30 seconds, 180 seconds, and 120 seconds, respectively.

Generally, the value of the garbage-collection timer is fixed to 4 times the value of the period update timer. Adjusting the period update timer will affect the garbage-collection timer.

The modification of RIP timers takes effect immediately.

Related Command: **display rip**

Example

Set the values of the Period Update timer and the Timeout timer of RIP to 10 seconds and 30 seconds respectively.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]rip
[4500-rip]timers update 10 timeout 30
```

IP Routing Policy Configuration Commands

This section describes the commands you can use to configure IP Routing Policy. These commands operate across all routing protocols.

When the Switch 4500 runs a routing protocol, it is able to perform the functions of a router. The term router in this section can refer either to a physical router or to the Switch 4500 running a routing protocol.

apply cost

Syntax

apply cost ***value***

undo apply cost

View

Route Policy View

Parameter

value Enter the route cost value of route information.

Description

Use the **apply cost** command to configure the route cost value of route information. This command is one of the **apply** sub-statements of the Route-policy attribute set.

Use the **undo apply cost** command to cancel the apply sub-statement.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, and **route-policy**.

Example

Define one **apply** sub-statement. When it is used for setting route information attribute, it sets the route metric value of route information to 120.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]route-policy permit node 1
   % New sequence of this list
[4500-route-policy]apply cost 120
```

display ip ip-prefix

Syntax

display ip ip-prefix [*ip_prefix_name* **]**

View

All views

Parameter

ip_prefix_name Enter displayed address prefix list name.

Description

Use the **display ip ip-prefix** command to view the address prefix list.

Related command: **ip ip-prefix**.

Example

Display the information of the address prefix list named to ***p1***.

```
<4500>display ip ip-prefix p1
name    index   conditions  ip-prefix / mask    GE  LE
p1      10      permit      10.1.0.0/16         17  18
```

Table 23 Output Description of the **display ip-ip prefix** Command

Field	Description
name	Name of ip-prefix
index	Internal sequence number of ip-prefix
conditions	Mode: permit or deny
ip-prefix	Address and network segment length of ip-prefix
GE	Greater-equal value of ip-prefix network segment length
LE	Less-equal value of ip-prefix network segment length

display route-policy

Syntax

display route-policy [*route_policy_name* **]**

View

All views

Parameter

route_policy_name Specify displayed Route-policy name.

Description

Use the **display route-policy** command to view the configured Route-policy

Related command: **route-policy**.

Example

Display the information of Route-policy named as policy1.

```
<4500>display route-policy policy1
Route-policy : policy1
  Permit 10 : if-match (prefixlist) p1
              apply cost 100
              matched : 0     denied : 0
```

Table 24 Output Description of the **display route-policy** Command

Field	Description
Route-policy	Name of ip-prefix
Permit 10	Information of the route-policy with mode as permit and node as 10: ■ if-match (prefixlist) p1 — The configured if-match clause ■ apply cost 100 — Apply routing cost 100 to the routes matching the conditions defined by if-match clause ■ matched — Number of routes matchng the conditions set by if-match clause ■ denied — Number of routes not matching the conditions set by if-match clause

if-match { acl | ip-prefix }

Syntax

if-match { acl *acl_number* | **ip-prefix** *ip_prefix_name* **}**

undo if-match [acl | **ip-prefix]**

View

Route policy view

Parameter

acl_number Enter the number of the access control list used for filtration

ip_prefix_name Enter the prefix address list used for filtration

Description

Use the **if-match { acl** | **ip-prefix }** command to configure the IP address range to match the Route-policy.

Use the **undo if-match { acl** | **ip-prefix }** command to cancel the setting of the match rule.

Filtration is performed by quoting an ACL or a prefix address list.

Related command: **if-match interface**, **if-match ip next-hop**, **if-match cost**, **route-policy**, **apply cost**.

Example

Define one **if-match** sub-statement. When the sub-statement is used for filtering route information, the route information filtered by the route destination address through address prefix list p1 can pass the **if-match** sub-statement.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]route-policy permit node 1
   % New sequence of this list
[4500-route-policy]if-match ip-prefix p1
```

if-match cost

Syntax

if-match cost *value*

undo if-match cost

View

Route policy view

Parameter

value Specify the required route metric value, ranging from 0 to 4294967295.

Description

Use the **if-match cost** command to configure one of the match rules of route-policy to match the cost of the routing information.

Use the **undo if-match cost** command to cancel the configuration of the match rule.

By default, no match sub-statement is defined.

Related commands: i**f-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match tag**, **route-policy**, **apply ip next-hop, apply local-preference, apply cost, apply origin** and **apply tag**.

Example

A match sub-statement is defined, which allows the routing information with routing cost 8 to pass this match sub-statement.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]route-policy permit node 1
   % New sequence of this list
[4500-route-policy]if-match cost 8
```

if-match interface

Syntax

if-match interface { *interface_name* | *interface_type interface_number* **}**

undo if-match interface

View

Route policy view

Parameter

interface_type Enter interface type.

interface_number Enter interface number.

interface_name Enter interface name.

Description

Use the **if-match interface** command to match the route whose next hop is the designated interface.

Use the **undo if-match interface** command to cancel the setting of matching condition.

By default, no match sub-statement is defined.

Related command: **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **route-policy**, **apply cost.**

Example

Define one match sub-statement to match the route whose next hop interface is Vlan-interface 1.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]route-policy permit node 1
   % New sequence of this list
[4500-route-policy]if-match interface Vlan-interface 1
```

if-match ip next-hop

Syntax

if-match ip next-hop { acl *acl_number* | **ip-prefix** *ip_prefix_name* **}**

undo if-match ip next-hop [ip-prefix]

View

Route policy view

Parameter

acl_number Enter the number of the access control list used for filtration. The range is 1 to 99.

ip_prefix_name Enter the name of the prefix address list used for filtration.

Description

Use the **if-match ip next-hop** command to configure one of the match rules of route-policy on the next hop address of the routing information.

Use the **undo if-match ip next-hop** command to cancel the setting of the ACL matching condition. Use the **undo if-match ip next-hop ip-prefix** command to cancel the setting of the address prefix list matching condition.

Filtration is performed by quoting an ACL or a address prefix list.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match cost**, **route-policy**, **apply cost.**

Example

Define a match sub-statement. It permits the routing information, whose route next hop address passes the filtration of the prefix address list p1, to pass this match sub-statement.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]route-policy permit node 1
   % New sequence of this list
[4500-route-policy]if-match ip next-hop ip-prefix p1
```

ip ip-prefix

Syntax

ip ip-prefix *ip_prefix_name* **[index** *index_number* **] { permit** | **deny }** *network len* **[greater-equal** *greater_equal* | **less-equal** *less_equal* **]**

undo ip ip-prefix *ip_prefix_name* **[index** *index_number* | **permit** | **deny]**

View

System view

Parameter

ip_prefix_name Enter the specified address prefix list name. It identifies one address prefix list uniquely.

index_number Identify an item in the prefix address list. The item with smaller index-number will be tested first.

permit Enter to specify the match mode of the defined address prefix list items as permit mode.

deny Enter to specify the match mode of the defined address prefix list items as deny mode.

network Enter the IP address prefix range (IP address). If it is 0.0.0.0 0, all the IP addresses are matched.

len Enter the IP address prefix range (mask length). If it is 0.0.0.0 0, all the IP addresses are matched.

greater_equal, less_equal The address prefix range [greater-equal, less-equal] to be matched after the address prefix network len has been matched. The meaning of **greater-equal** is "larger than or equal to" , and the meaning of **less-equal** is "less than or equal to". The range is len <= greater-equal <= less-equal <= 32. When only **greater-equal** is used, it denotes the prefix range [greater-equal, 32]. When only **less-equal** is used, it denotes the prefix range [len, less-equal].

Description

Use the **ip ip-prefix** command to configure an address prefix list or one of its items.

Use the **undo ip ip-prefix** command to delete an address prefix list or one of its items.

By default, there's no address prefix list.

The address prefix list is used for IP address filtering. An address prefix list may contain several items, and each item specifies one address prefix range. The inter-item filtering relation is "OR", i.e. passing an item means passing the filtering of this address prefix list. Not passing the filtering of any item means not passing the filtration of this prefix address list.

The address prefix range may contain two parts, which are determined by ***len*** and [*greater-equal, less-equal*] respectively. If the prefix ranges of these two parts are both specified, the IP to be filtered must match the prefix ranges of these two parts.

If you specify ***network len*** as 0.0.0.0 0, it only matches the default route.

Example

The prefix address list of this address indicates to match the bits 1 to 8 and the bits 17 to 18 for filtering the IP address with the bits 1 to 8 and the bits 17 to 18 of the specified IP network segment 10.0.192.0.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]ip ip-prefix p1 permit 10.0.192.0 8 greater-equal 17
less-equal 18
```

route-policy

Syntax

route-policy *route_policy_name* **{ permit** | **deny } node {** *node_number* **}**

undo route-policy *route_policy_name* **[permit** | **deny** | **node** *node_number* **]**

View

System view

Parameter

route_policy_name Enter the Route-policy name to identify one Route-policy uniquely.

permit Enter to specify the match mode of the defined Route-policy node as permit mode.

deny Enter to specify the match mode of the defined Route-policy node as deny mode.

node Enter the node of the route policy.

node_number Enter the index of the node in the route-policy. When this route-policy is used for routing information filtration, the node with smaller node-number will be tested first.

Description

Use the **route-policy** command to create and enter the Route-policy view.

Use the **undo route-policy** command to delete the established Route-policy.

By default, no Route-policy is defined.

The **route-policy** command is used for route information filtration or route policy. One Route-policy comprises some nodes and each node comprises some match and apply sub-statements. The match sub-statement defines the match rules of this node and the apply sub-statement defines the actions after passing the filtration of this node. The filtering relationship between the match sub-statements of the node is “and”, that is, all match sub-statements that meet the node. The filtering relation between Route-policy nodes is "OR", i.e. passing the filtering of one node means passing the filtering of this Route-policy. If the information does not pass the filtration of any nodes, it cannot pass the filtration of this Route-policy.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **apply cost**.

Example

Configured one Route-policy policy1, whose node number is 10 and if-match mode is permit, and enter Route policy view.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]route-policy policy permit node 10
   % New sequence of this list
```

```
[4500-route-policy]
```

7 USING MULTICAST PROTOCOL COMMANDS

This chapter describes how to use the following commands:

IGMP Snooping Configuration Commands

- display igmp-snooping configuration
- display igmp-snooping group
- display igmp-snooping statistics
- igmp-snooping
- igmp-snooping host-aging-time
- igmp-snooping max-response-time
- igmp-snooping router-aging-time
- reset igmp-snooping statistics

IGMP Snooping Configuration Commands

This section describes how to use the Internet Group Management Protocol (IGMP) configuration commands on your Switch 4500.

display igmp-snooping configuration

Syntax

display igmp-snooping configuration

View

All views

Parameter

None

Description

Use the **display igmp-snooping configuration** command to view the IGMP Snooping configuration information.

This command is used to display the IGMP Snooping configuration information of the Switch. The information displayed includes whether IGMP Snooping is enabled, router port timeout, maximum response timeout of a query and the member port timeout.

Related command: **igmp-snooping.**

Example

Display the IGMP Snooping configuration information of the Switch.

```
<4500>display igmp-snooping configuration
Enable IGMP-Snooping.
The router port timeout is 300 second(s).
The max response timeout is 50 second(s).
The member port timeout is 500 second(s).
```

The information above tells us that: IGMP Snooping is enabled; the router port timer is set to be 300 seconds; the max response timer is set to be 50 seconds; the aging timer of multicast group member is set to be 500 seconds.

display igmp-snooping group

Syntax

display igmp-snooping group [vlan *vlan_id*]

View

All views

Parameter

vlan *vlan_id*: Specifies the VLAN where the multicast group to be viewed is located. When the parameter is omitted, the command will display the information about all the multicast groups on the VLAN.

Description

Use the **display igmp-snooping group** command to view the IP multicast groups and MAC multicast groups under VLAN.

This command displays the IP multicast group and MAC multicast group information of a VLAN or all the VLAN where the Ethernet Switch is located. It displays the information such as VLAN ID, router port, IP multicast group address, member ports in the IP multicast group, MAC multicast group, MAC multicast group address, and the member ports in the MAC multicast group.

Example

Display the multicast group information about VLAN2.

```
<4500>display igmp-snooping group vlan 2
***************Multicast group table***************
Vlan(id):2.
Router port(s):Ethernet1/0/1
IP group(s):the following ip group(s) match to one mac group.
IP group address:230.45.45.1
Member port(s):Ethernet1/0/2
MAC group(s):
MAC group address:01-00-5e-2d-2d-01
Member port(s):Ethernet1/0/2
```

The display above shows that:

- There is a multicast group in VLAN 2;
- The router port is Ethernet 1/0/1;
- The address of the multicast group is 230.45.45.1;
- The member of the IP multicast group is Ethernet 1/0/2;
- MAC multicast group is 0100-5e2d-2d01;
- The member of the MAC multicast group is Ethernet 1/0/2

display igmp-snooping statistics

Syntax

display igmp-snooping statistics

View

All views

Parameter

None

Description

Use the **display igmp-snooping statistics** command to view the statistics information on IGMP Snooping.

This command displays the statistics information about IGMP Snooping of the Ethernet Switch. It displays the information such as number of received general IGMP query packets, received IGMP specific query packets, received IGMP Version 1 and Version 2 report packets, received IGMP leave packets and error packets, and sent IGMP specific query packets.

Related command: **igmp-snooping**.

Example

Display statistics information about IGMP Snooping.

```
<4500>display igmp-snooping statistics
Received IGMP general query packet(s) number:0.
Received IGMP specific query packet(s) number:0.
Received IGMP V1 report packet(s) number:0.
Received IGMP V2 report packet(s) number:0.
Received IGMP leave packet(s) number:0.
Received error IGMP packet(s) number:0.
Sent IGMP specific query packet(s) number:0.
```

igmp-snooping

Syntax

igmp-snooping { enable | disable }

View

System View

Parameter

enable: Enable IGMP Snooping.

disable: Disables IGMP Snooping; By default, the Switch disables IGMP Snooping feature.

Description

Use the **igmp-snooping enable** command to enable/disable IGMP Snooping.

Use the **igmp-snooping disable** command to restore the default setting.

Although layer 2 and layer 3 multicast protocols can run together, they cannot run on the same VLAN or its corresponding VLAN interface at the same time. For example, if the layer 2 multicast protocol is enabled on a VLAN, then the layer 3 multicast protocol cannot operate on this VLAN, and vice versa.

IGMP Snooping functions only when it is enabled both in System View and in VLAN View. You must first enable IGMP Snooping globally in System View and then the VLAN View before configuring it. Otherwise, the IGMP Snooping fails to operate.

Example

Enable IGMP Snooping on VLAN 100.

```
<4500>system-view
System View: return to User View with Ctrl+Z
[4500]igmp-snooping enable
[4500]vlan 100
[4500-vlan100]igmp-snooping enable
```

igmp-snooping host-aging-time

Syntax

igmp-snooping host-aging-time *seconds*

undo igmp-snooping host-aging-time

View

System View

Parameter

seconds: Specifies the port aging time of the multicast group member, ranging from 200 to 1000 and measured in seconds. The default is 260.

Description

Use the **igmp-snooping host-aging-time** command to configure the port aging time of the multicast group members.

Use the **undo igmp-snooping host-aging-time** command to restore the default value.

This command sets the aging time of the multicast group member so that the refresh frequency can be controlled. When the group members change frequently, the aging time should be comparatively short, and vice versa.

Related command: **igmp-snooping**.

Example

Set the aging time to 300 seconds.

```
<4500>system-view
System View: return to User View with Ctrl+Z
[4500]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

Parameter

seconds: Maximum response time for a query ranging from 1 to 25 and measured in seconds. The default is 10.

Description

Use the **igmp-snooping max-response-time** command to configure the maximum response time for a query.

Use the **undo igmp-snooping max-response-time** command to restore the default value.

The set maximum response time decides the time limit for the Switch to respond to IGMP Snooping general query packets.

Related commands: **igmp-snooping**, **igmp-snooping router-aging-time**.

Example

Configure to respond to the IGMP Snooping packet within 20s.

```
<4500>system-view
System View: return to User View with Ctrl+Z
```

```
[4500]igmp-snooping max-response-time 20
```

igmp-snooping router-aging-time

Syntax

igmp-snooping router-aging-time ***seconds***

undo igmp-snooping router-aging-time

View

System View

Parameter

seconds: Specifies the router port aging time, ranging from 1 to 1000 measured in seconds. The default is 105.

Description

Use the **igmp-snooping router-aging-time** command to configure the router port aging time of IGMP Snooping.

Use the **undo igmp-snooping router-aging-time** command to restore the default value.

The port here refers to the Switch port connected to the router. The Layer-2 Ethernet Switch receives general query packets from the router via this port. The timer should be set to about 2.5 times of the general query period of the router.

Related commands: **igmp-snooping**, **igmp-snooping max-response-time**.

Example

Set the aging time of the IGMP Snooping router port to 500 seconds.

```
<4500>system-view
System View: return to User View with Ctrl+Z
[4500]igmp-snooping router-aging-time 500
```

reset igmp-snooping statistics

Syntax

reset igmp-snooping statistics

View

User View

Parameter

None

Description

Use the **reset igmp-snooping statistics** command to reset the IGMP Snooping statistics information.

Related command: **igmp-snooping**.

Example

Clear IGMP Snooping statistics information.

```
<4500>reset igmp-snooping statistics
```

8 USING QOS/ACL COMMANDS

This chapter describes how to use the following commands:

ACL Commands List

- acl
- display acl
- display packet-filter
- packet-filter
- reset acl counter
- rule

QoS Configuration Commands List

- display mirror
- display qos cos-local-precedence- map
- display qos-interface all
- display qos-interface line-rate
- display qos-interface mirrored-to
- display qos-interface traffic-limit
- line-rate
- mirrored-to
- mirroring-port
- monitor-port
- priority
- priority trust
- qos cos-local-precedence -map
- traffic-limit
- wred

Logon user's ACL Control Command

- acl
- ip http acl
- snmp-agent community
- snmp-agent group
- snmp-agent usm-user

ACL Commands List

This section describes how to use the ACL configuration commands on your Switch 4500.

acl

Syntax

```
acl acl-number1 { inbound | outbound }
undo acl acl-number1 { inbound | outbound }
acl acl-number2 inbound
undo acl acl-number2 inbound
```

View

```
User interface view
```

Parameter

```
acl-number1: Number of number-based basic and advanced ACLs, in the
range of 2,000 to 3,999.
acl-number2: Number of number-based L2 ACLs, in the range of 4,000 to
4,999.
inbound: Implements ACL control over the users logging into local
switch in the TELNET or SSH mode.
outbound: Implements ACL control over the users logging into other
switches from local switch in the TELNET or SSH mode.
```

Description

Use the acl command to use ACLs, implementing ACL control over TELNET or SSH users.

Use the undo acl command to cancel the ACL control over TELNET or SSH users.

- *You can only use number-based ACLs for TELNET or SSH user ACL control.*
- *When TELNET or SSH users use basic or advanced ACLs, the incoming/outgoing calls are restricted on the basis of the source or destination IP address. As a result, when you use the rules for basic and advanced ACLs, only the source IP and the corresponding mask, the destination IP and the corresponding mask, and the time-range keyword take effect. When TELNET and SSH users use L2 ACLs, the incoming/outgoing calls are restricted on the basis of source MAC addresses. As a result, when you use the rules for L2 ACLs, only the source MAC and the corresponding mask, and the time-range keyword take effect.*
- *When you control telnet and SSH users on the basis of L2 ACLs, only the incoming calls are restricted.*
- *If a user is refused to log in due to ACL restriction, the system will record the log information about an access failure. The log information includes the user IP address, login mode, index value for a login user interface and reason for login failure.*

By default, the incoming/outgoing calls of the user interface are not restricted.

Example

Implement ACL control over users logging into local switch in the TELNET mode. (You have defined basic ACL 2000)

```
<4500>system-view
System View: return to User View with Ctrl+Z.
```

```
[4500] user-interface vty 0 4
[4500-user-interface-vty0-4] acl 2000 inbound
```

display acl

Syntax

display acl { all | ***acl-number*** **}**

View

All views

Parameter

all: Displays all ACLs.

acl-number: Specifies the sequence number of the ACL to be displayed. It can be a number chosen from 2000 to 5999.

Description

Use the **display acl** command to view the detailed configuration information about the ACL, including every rule, sequence number and the number and byte number of the packets matched with this rule.

The matched times displayed by this command are software matched times, namely, the matched times of the ACL to be processed by the Switch CPU.

Example

Display the content of all the ACLs.

```
<4500>display acl all
Basic acl 2000, 0 rule,match-order is auto
Acl’s step is 1

Advanced ACL  3000, 1 rule
Acl's step is 1
 rule 1 permit ip (0 times matched)
```

display packet-filter

Syntax

display packet-filter { interface { ***interface-name*** | ***interface-type interface-num*** **}** | **unitid** ***unit-id*** **}**

View

Any view

Parameter

interface { ***interface-name*** | ***interface-type interface-num*** **}:** Interface of the Switch, for more detail, please refer to the **port** command in this guide.

unitid ***unit-id*****:** Unit ID. If user inputs this parameter, all the packet-filtering information of the specified unit will be displayed.

Description

Use the **display packet-filter** command to view the information of the packet filter function. The displayed content includes ACL number, subitem name and activation status.

Example

To display the information of the activated ACL of all interfaces, enter the following:

```
<4500>display packet-filter unitid 1
```

packet-filter

Syntax

packet-filter { inbound | outbound } { user-group *acl-number* [rule *rule*] | ip-group *acl-number* [rule *rule* [link-group *acl-number* rule *rule*]] | link-group *acl-number* [rule *rule*] }

undo packet-filter { inbound | outbound } { user-group *acl-number* [rule *rule*] | ip-group *acl-number* [rule *rule* [link-group *acl-number* rule *rule*]] | link-group *acl-number* [rule *rule*] }

View

Ethernet Port View.

Parameter

inbound: Filters the traffic received by the Ethernet port.

outbound: Performs filtering to the packets sent by the interface.

user-group *acl-number*: Activates user-defined ACLs. ***acl-number***: Sequence number of the ACL, ranging from 5000 to 5999.

ip-group *acl-number*: Activates the IP ACLs, including basic and advanced ACLs. ***acl-number*** specifies the sequence number of the ACL, ranging from 2000 to 3999.

link-group *acl-number*: Activates the Layer 2 ACLs. ***acl-number*** specifies the ACL number, ranging from 4000 to 4999.

rule *rule*: Specifies the rule of an ACL, ranging from 0 to 65534; if not specified, all subitems of the ACL will be activated. An ACL can have many rules. They start at 0.

Description

Use the **packet-filter** command to activate the ACL on a specific interface.

Use the **undo packet-filter** command to disable the ACL on a specific interface.

Example

Activate ACL 2000 for inbound traffic on interface Ethernet 1/0/1.

```
<4500>system-view
System View: return to User View with Ctrl+Z
[4500]interface Ethernet 1/0/1
[4500-Ethernet1/0/1]packet-filter inbound ip-group 2000
[4500-Ethernet1/0/1]
```

reset acl counter

Syntax

reset acl counter { all | *acl-number* }

View

User View

Parameter

all: All ACLs.

***acl-number*:** Specifies the sequence number of an ACL.

Description

Use the **reset acl counters** command to reset the ACL statistics information to zero.

Example

Clear the statistics information of ACL 2000.

```
<4500>reset acl counters 2000
```

rule

Syntax

Define or delete the subrules of a basic ACL:

rule [*rule-id*] { permit | deny } [source { *source-addr wildcard* | any } fragment]*

undo rule *rule-id* [source | fragment]*

Define or delete the subrules of an advanced ACL:

rule [*rule-id*] { permit | deny } *protocol* [source { *source-addr wildcard* | any }] [destination { *dest-addr wildcard* | any }] [source-port *operator port1* [*port2*]] [destination-port *operator port1* [*port2*]] [icmp-type *type code*] [established] [[{ precedence *precedence* tos *tos* }* | dscp *dscp*] [vpn-instance *instance* | fragment]*

undo rule *rule-id* [source | destination | source-port | destination-port | icmp-type | precedence | tos | dscp | fragment | time-range | vpn-instance]*

Define or delete the subrules of a Layer 2 ACL:

rule [*rule-id*] { permit | deny } [[type *protocol-type type-mask* | lsap */sap-type type-mask*] | *format-type* | cos *cos* | source { *source-vlan-id* / *source-mac-addr source-mac-wildcard* }* | dest { *dest-mac-addr dest-mac-wildcard* }]*

undo rule *rule-id*

Define or cancel the subrules of user-defined ACL

rule [*rule-id*] { permit | deny } { *rule-string rule-mask offset* }&<1-8>]

undo rule *rule-id*

View

Corresponding ACL View

Parameter

rule-id: Specifies the subitems of an ACL, ranging from 0 to 65534.

permit: Permits packets that meet the requirements.

deny: Denies packets that meet the requirements.

The following parameters are various property parameters carried by packets. The ACL sets rules according to this parameter.

Parameters specific to basic ACLs:

source { *source-addr wildcard* | any }: ***source-addr wildcard*** represents the source IP address and the wildcard digit represented in dotted decimal notation. **any** represents all source addresses.

fragment: Means this rule is only effective fragment packets and is ignored for non-fragment packets.

Parameters specific to advanced ACLs:

protocol: Specifies the protocol type which is represented by a name or a number. When it is a name, this parameter can be adopted like: icmp, igmp, tcp, udp, ip, gre, ospf, ipinip, etc. If the adopted value is IP, that means all the Internet Protocols. When it is a number: it ranges from 1 to 225.

source { *source-addr wildcard* | any }: ***source-addr wildcard*** means the source IP address and the wildcard digit represented in dotted decimal notation. **any** means all source addresses.

destination { *dest-addr wildcard* | any }: ***dest-addr wildcard*** means the destination IP address and the wildcard digit represented in dotted decimal notation. **any** means all destination addresses.

source-port *operator port1 [port2]*: Source port number of TCP or UDP used by the packet. ***operator*** is port operator, including eq (equal), gt (greater than), lt (less than),neq (not-equal), range (within this range). Note that this parameter is only available when the parameter *protocol* is TCP or UDP. *port1* [*port2*]: Source port number of TCP or UDP used by the packet, notated by a character or a number which ranges from 0 to 65535 inclusive. For the value of the character, please refer to mnemonic symbol table. The two parameters *port1* and *port2* appear at the same time only when the operator is "range", but other operators need "*port1*" only.

destination-port *operator port1 [port2*]: Destination port number of TCP or UDP used by packets. For detailed description, please refer to **source-port *operator port1 [port2]***.

icmp-type *type code*: Appears when *protocol* is icmp. ***type code*** specifies an ICMP packet. ***type*** represents the type of ICMP packet, notated by a character or

a number which ranges from 0 to 255; ***code*** represents ICMP code, which appears when the protocol is "icmp" and the type of packet is not notated by a character, ranging from 0 to 255.

established: Means that it is only effective to the first SYN packet established by TCP, appears when *protocol* is TCP.

precedence ***precedence***: IP precedence, can be a name or a number ranging from 0 to 7.

tos ***tos***: ToS (Type of Service) value, can be a name or a number ranging from 0 to 15. Packets can be classified according to TOS value.

dscp ***dscp***: DSCP (Differentiated Services Code Point) value, can be a name or a number ranging from 0 to 63. Packets can be classified according to DSCP value.

fragment: Means this rule is only effective for fragment packets and is ignored for non-fragment packets.

Parameters specific to Layer 2 ACL:

source ***{ source-vlan-id*** | ***source-mac-addr source-mac-wildcard }****: The source information of a packet, ***source-vlan-id*** represents source VLAN of the packet, ***source-mac-addr source-mac-wildcard*** represents source MAC address of the packet. For example, if you set ***source-mac-wildcard*** to 0-0-ffff, it means that you will take the last 16 bits of source MAC address as the rule of traffic classification.

dest ***{ dest-vlan-id*** | ***dest-mac-addr dest-mac-wildcard }****: The destination information of a packet: ***dest-mac-addr dest-mac-wildcard*** represents the packet's destination MAC address. For example, if you set ***source-mac-wildcard*** to 0-0-ffff, it means that you will take the last 16 bits of source MAC address as the rule of traffic classification.

type ***protocol-type protocol-type-mask***: Protocol type carried by the Ethernet frame.

lsap ***lsap-type lsap-type-mask***: lsap type carried by the Ethernet frame.

The parameter for user-defined ACL

{ rule-string rule-mask offset }&<1-8>: ***rule-string*** is a character string of a rule defined by a user ranging from 2 to 80 characters. It is a hexadecimal string with even digits. ***rule-mask offset*** is used to extract the packet information. Here, ***rule-mask*** is ***rule mask***, used for logical AND operation with data packets, and ***offset*** determines to perform AND operation from which bytes apart from the packet header. ***rule-mask offset*** extracts a character string from the packet and compares it with the user-defined rule-string to get and process the matched packets. ***&<1-8>*** indicates that you can define up to 8 such rules at a time. This parameter is used for the user-defined ACL.

Description

Use the **rule** command to add a subrule to an ACL.

Use the **undo rule** command to cancel a subrule from an ACL.

You can define several subrules for an ACL. If you include parameters when using the **undo rule** command, the system only deletes the corresponding content of the subrule.

For related configurations, refer to command **acl**.

Example

Add a subrule to an advanced ACL:

```
<4500>system-view
System View: return to User View with Ctrl+Z
[4500]acl number 3000
[4500-acl-adv-3000]rule 1 permit tcp established source 1.1.1.1 0
destination 2.2.2.2 0
```

Add a subrule to a basic ACL:

```
<4500>system-view
System View: return to User View with Ctrl+Z
[4500]acl number 2000
[4500-acl- basic-2000]rule 1 permit source 1.1.1.1 0 fragment
```

Add a subrule to a Layer 2 ACL:

```
<4500>system-view
System View: return to User View with Ctrl+Z
[4500]acl number 4000
[4500-acl-ethernetframe-4000] rule 1 permit source 1
```

Add a rule to a user-defined ACL:

```
<4500>system-view
System View: return to User View with Ctrl+Z
[4500]acl number 5000
[4500-acl-user-5000] rule 1 permit 88 ff 18
```

QoS Configuration Commands List

This section describes how to use the Quality of Service (QoS) configuration commands on your Switch 4500.

display mirror

Syntax

display mirror

View

Any view

Parameter

None

Description

Use the **display mirror** command to view port mirroring configuration, including monitored ports, monitor port and monitor direction, and so on.

Related commands: **mirroring-port**, **monitor-port**.

Example

To display the port mirroring configuration, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z
[4500] display mirror
```

display qos cos-local-precedence-map

Syntax

display qos cos-local-precedence-map

View

All views

Parameter

None

Description

Use the **display qos cos-local-precedence-map** command to view COS and Local-precedence map.

Example

Display COS and Local-precedence map.

```
<4500>display qos cos-local-precedence-map
cos-local-precedence-map:
 802.1p & local precedence : 0     1     2     3     4     5     6     7
-------------------------------------------------------------------------
                      queue: 2     0     1     3     4     5     6     7
```

display qos-interface all

Syntax

display qos-interface { *interface-name* | *interface-type interface-num* | *unit-id* } all

View

All views

Parameter

interface-name | ***interface-type interface-num***: Interfaces of the Switch. For more information, refer to the **port** command in this guide.

unit-id: Unit ID of the Switch.

Description

Using the **display qos-interface { *interface-name* | *interface-type interface-num* | *unit-id* } all** command, you can view QoS information of all interfaces. If you do not input interface parameters, this command will display all QoS setting information for the Switch, including traffic policing, rate limit at interface, and so on. If you input interface parameters, this command will display

QoS setting information of the specified interfaces, including traffic policing, rate limit at interfaces, and so on.

Example

Display all the configurations of QoS parameters for unit 1.

```
<4500> display qos-interface 1 all
```

display qos-interface line-rate

Syntax

display qos-interface { *interface-name* | *interface-type interface-num* | *unit-id* } line-rate

View

Any view

Parameter

interface-name* | *interface-type interface-num: Interface of the Switch, for detailed a description, refer to the **port** command in this guide.

unit-id: Unit ID of the Switch.

Description

Use the **display qos-interface line-rate** command to view the traffic rate limitations of the interface output. If you do not specify interface parameters, you will view the traffic rate limitations of all interfaces' output. If you enter interface parameters, you will view the parameter settings of traffic rate limitations of the specified interfaces' output.

Example

Display the parameter configuration of interface traffic rate limitation.

```
<4500>system-view
System View: return to User View with Ctrl+Z
[4500] display qos-interface line-rate
Ethernet1/0/1: line-rate
   Outbound: 128 kbps
```

display qos-interface mirrored-to

Syntax

display qos-interface { *interface-name* | *interface-type interface-num* | *unit-id* } mirrored-to

View

Any view

Parameter

***interface-name* | *interface-type interface-num*:** Interface of the Switch, for detailed description, refer to the **port** command in this guide.

***unit-id*:** Unit ID of the Switch.

Description

Use the **display qos-interface mirrored-to** command to view the settings of the traffic mirror.

This command is used for displaying the settings of traffic mirror. The information displayed includes the ACL of traffic to be mirrored and the observing port.

Related command: **mirrored-to**.

Example

To display the settings of traffic mirror, enter the following:

```
<4500> display qos-interface ethernet1/0/1 mirrored-to
Ethernet1/0/1: mirrored-to
 Inbound:
   Matches: Acl 2000 rule 0  running
     Mirrored to: monitor interface
```

display qos-interface traffic-limit

Syntax

display qos-interface { ***interface-name*** | ***interface-type interface-num*** | ***unit-id*** } **traffic-limit**

View

All views

Parameter

interface-name | ***interface-type interface-num***:: Specifices an Interface of the Switch, for more information, refer to the **port** command in this guide.

unit-id: Unit ID of the Switch.

Description

Use the **display qos-interface traffic-limit** command to view the traffic limit settings. If you set the port parameters, the configuration information about the specified port will be displayed. The information displayed includes the ACL of the traffic to be limited, the limited average rate and the settings of some related policing action.

Related commands: **traffic-limit.**

Example

Display the traffic limit settings.

```
<4500> display qos-interface ethernet1/0/1 traffic-limit
Ethernet1/0/1: traffic-limit
 Inbound:
   Matches: Acl 2000 rule 0  running
     Target rate: 128 Kbps
     Exceed action: remark-dscp 63
```

line-rate

Syntax

line-rate ***target-rate***
undo line-rate

View

Ethernet Port View

Parameter

***target-rate*:** The total limited rate of the packets sent by interfaces. Unit in Kbps. The number input must be a multiple of 64. For 100 Mbps port, the range is from 64 to 99968; for 1000 Mbps port, the range is from 64 to 1000000.

Description

Use the **line-rate** command, to limit the total rate of the packets received or delivered by interfaces. Use the **undo line-rate** command, to cancel the configuration of limit rate at interfaces.

The granularity of line rate is 64 kbps.

Example

Set the rate limitation of interface Ethernet1/0/1 to 128 kbps.

```
<4500>system-view
System View: return to User View with Ctrl+Z
[4500]interface Ethernet 1/0/1
[4500]line-rate outbound 128
```

mirrored-to

Syntax

mirrored-to { inbound | outbound } { user-group *acl-number* [rule *rule*] | ip-group *acl-number* [rule *rule* [link-group *acl-number* rule *rule*]] | link-group *acl-number* [rule *rule*] } { cpu | monitor-interface }

undo mirrored-to { inbound | outbound } { user-group *acl-number* [rule *rule*] | ip-group *acl-number* [rule *rule* [link-group *acl-number* rule *rule*]] | link-group *acl-number* [rule *rule*] }

View

Ethernet Port View

Parameter

inbound: Performs traffic mirror for the packets received by the interface.

outbound: Performs traffic mirror for the packets sent by the interface.

user-group *acl-number*: Activates user-defined ACLs. ***acl-number***: Sequence number of ACL, ranging from 5000 to 5999.

ip-group *acl-number*: Activates IP ACLs, including basic and advanced ACLs. ***acl-number*:** Sequence number of ACL, ranging from 2000 to 3999.

link-group *acl-number*: Activates Layer 2 ACLs. ***acl-number***: Sequence number of ACL, ranging from 4000 to 4999.

rule *rule*: Specifies the subitem of an active ACL, ranging from 0 to 65534; if not specified, all subitems of the ACL will be activated. If only IP ACL or Layer 2 ACL is activated, this parameter can be omitted. If both IP and Layer 2 ACL are activated at the same time, the ***rule*** parameter cannot be omitted.

cpu: Specifies the traffic will be mirror to CPU

monitor-interface: Specifies that the destination port is the monitor port.

Description

Use the **mirrored-to** command to enable ACL traffic identification and perform traffic mirroring.

Use the **undo mirrored-to** command to disable traffic mirroring.

This command is used for mirroring the traffic matching the specified ACL (whose action is permit). The observing port cannot be a Trunk port or aggregated port.

This command only supports one observing port. When you use the traffic mirror for the first time, you have to designate the observing port.

Related command: **display qos-interface mirrored-to**.

Example

To mirror the packets matching the ACL 2000 rules, whose action is permit, to the port Ethernet1/0/1, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z
[4500]interface Ethernet 1/0/1
[4500-Ethernet1/0/1]monitor-port
[4500-Ethernet1/0/1]quit
[4500]interface Ethernet 1/0/2
[4500-Ethernet1/0/2] mirrored-to ip-group 2000 monitor-interface
4500-Ethernet1/0/2]
```

mirroring-port

Syntax

mirroring-port { inbound | **outbound** | **both }**

undo mirroring-port

View

Ethernet Port View

Parameter

None.

Description

Use the **mirroring-port** command to configure a mirroring port.

Use the **undo mirroring-port** command to remove setting of mirroring port.

The Switch supports one monitor port and one mirroring port. If several Switches form a Fabric, only one monitor port and one mirroring port can be configured in

the Fabric. You need to configure the monitor port before configuring the monitored port.

Related command: **display mirror**.

Example

To configure Ethernet1/0/1 as a monitored port, and monitor packets in both directions, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z
[4500]interface Ethernet 1/0/1
[4500-Ethernet1/0/1] mirroring-port both
[4500-Ethernet1/0/1]
```

monitor-port

Syntax

monitor-port

undo monitor-port

View

Ethernet Port View

Parameter

None

Description

Use the **monitor-port** command to configure a monitor port.

Use the **undo monitor-port** command to remove the setting of monitor port.

The Switch supports one monitor port and one mirroring port. If several Switches form a Fabric, only one monitor port and one mirroring port can be configured in the Fabric. You need to configure monitor port before configuring monitored port.

Related command: **display mirror**.

Example

To configure the port Ethernet1/0/4 as a monitor port, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z
[4500]interface Ethernet 1/0/4
[4500-Ethernet1/0/4] monitor-port
[4500-Ethernet1/0/4]
```

priority

Syntax

priority ***priority-level***

undo priority

View

Ethernet Port View

Parameter

priority-level: Specifies the priority level of the port, ranging from 0 to 7.

Description

Use the **priority** command to configure the priority of Ethernet port.

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

By default, the priority level of the port is 0. The Switch replaces the 802.1p priority carried by a packet with the port priority that is defined.

Every port on the Switch supports eight packet egress queues. The Switch puts the packets into different egress queues according to their priorities.

When transmitting a packet, the Switch replaces the packet's 802.1p priority with the priority of the received port, according to which the packet will be put into the corresponding egress queue.

Example

Set the priority of Ethernet1/0/1 port to 7.

```
<4500>system-view
System View: return to User View with Ctrl+Z
[4500]interface Ethernet 1/0/1
[4500-Ethernet1/0/1]priority 7
[4500-Ethernet1/0/1]
```

priority trust

Syntax

```
priority trust
undo priority
```

View

Ethernet Port View

Parameter

None

Description

Use the **priority trust** command to configure the system to trust the packet's 802.1p priority and not replace the 802.1p priorities carried by the packets with the port priority. Use **undo priority** command to configure the system not to trust the packet 802.1p priority.

By default, the system replaces the 802.1p priority carried by a packet with the port priority.

For the related command, see **priority**.

Example

Configure the system to trust the packet 802.1p priority and not replace the 802.1p priorities carried by the packets with the port priority.

```
<4500>system-view
```

```
System View: return to User View with Ctrl+Z
[4500]interface Ethernet 1/0/1
[4500-Ethernet1/0/1]priority trust
[4500-Ethernet1/0/1]
```

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

Parameter

cos0-map-local-prec: CoS 0 -> Local precedence (queue) mapping value, in the range of 0~7.

cos1-map-local-prec: CoS 1 -> Local precedence (queue) mapping value, in the range of 0~7.

cos2-map-local-prec: CoS 2 -> Local precedence (queue) mapping value, in the range of 0~7.

cos3-map-local-prec: CoS 3 -> Local precedence (queue) mapping value, in the range of 0~7.

cos4-map-local-prec: CoS 4 -> Local precedence (queue) mapping value, in the range of 0~7.

cos5-map-local-prec: CoS 5 -> Local precedence (queue) mapping value, in the range of 0~7.

cos6-map-local-prec: CoS 6 -> Local precedence (queue) mapping value, in the range of 0~7.

cos7-map-local-prec: CoS 7 -> Local precedence (queue) mapping value, in the range of 0~7.

Description

Use the **qos cos-local-precedence-map** command to configure "CoS Local-precedence" mapping table. This will map a CoS value to a specific local precedence (queue). Note that traffic which has been assigned a local precedence via QOS will also be assigned to the same queue.

Use the **undo qos cos-local-precedence-map** command to restore its default values.

The following is the default CoS and Local Precedence table.

Table 25 Default CoS and Local-precedence table

Cos and Local Precedence Value	Local Precedence Queue
0	2
1	0
2	1

Cos and Local Precedence Value	Local Precedence Queue
3	3
4	4
5	5
6	6
7	7

Example

Configure CoS and Local Precedence table.

```
<4500>system-view
System View: return to User View with Ctrl+Z
[4500]qos cos-local-precedence-map 0 1 2 3 4 5 6 7
[4500]
```

The following is the configured "CoS Local-precedence" mapping table.

Table 26 Default configure CoS and Local-precedence table

Cos and Local Precedence Value	Local Precedence Queue
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

traffic-limit

traffic-limit inbound { **user-group** ***acl-number*** [**rule** ***rule***] | **ip-group** ***acl-number*** [**rule** ***rule*** [**link-group** ***acl-number*** **rule** ***rule***]] | **link-group** ***acl-number*** [**rule** ***rule***] } ***target-rate*** [**exceed** ***action***]

undo traffic-limit inbound { **user-group** { ***acl-number*** [**rule** ***rule***] | **ip-group** ***acl-number*** [**rule** ***rule*** **[link-group** ***acl-number*** **rule** ***rule*** **]** **]** | **link-group** ***acl-number*** **[rule** ***rule*** **]** **}**

View

Ethernet Port View

Parameter

inbound: Performs traffic limitation to the packets received by the interface.

user-group ***acl-number***: Activates user-defined ACLs. ***acl-number***: Sequence number of ACL, ranging from 5000 to 5999.

ip-group ***acl-number***: Activates IP ACLs, including basic and advanced ACLs. ***acl-number*** : Sequence number of ACL, ranging from 2000 to 3999.

link-group *acl-number*: Activates Layer 2 ACLs. acl-number: Sequence number of ACL, ranging from 4000 to 4999.

rule *rule*: Specifies the subitem of an active ACL, ranging from 0 to 65534; if not specified, all subitems of the ACL will be activated. If only an IP ACL or a Layer 2 ACL is activated, this parameter can be omitted. If both IP and Layer 2 ACLs are activated at the same time, the ***rule*** parameter cannot be omitted.

target-rate: The set normal traffic, unit in Kbps, the granularity of traffic limit is 64 kbps, if the number input is in (N*64 <the number input<(N+1)*64), in which N is a natural number, the Switch automaticaly sets (N+1)*64 as the parameter value. For 100 Mbps ports, ***target-rate*** ranges from 64 to 99968 inclusive; for 1000 Mbps ports, from 64 to 1000000 inclusive.

exceed *action*: The action taken when the traffic exceeds the threshold. The ***action*** can be:

- ***drop***: Drops the packets.
- ***remark-dscp value***: Sets new DSCP value.

Description

Use the **traffic-limit** command, to activate the ACL and perform traffic limitation. Use the **undo traffic-limit** command to remove traffic limitation.

This command performs traffic limitation on the packets that match with a specified ACL rule, and is only effective with a permit rule.

The granularity of traffic limit is 64 kbps.

You can only remark traffic with a DSCP value. The Switch 4500 does not permit CoS remarking with this command.

Example

Perform traffic limitation on packets that match the permit rule of ACL 2000. The target traffic rate is 128 kbps.

```
<4500>system-view
System View: return to User View with Ctrl+Z
[4500]interface Ethernet 1/0/1
[4500-Ethernet1/0/1] traffic-limit inbound ip-group 2000 128
[4500-Ethernet1/0/1]
```

wred

Syntax

wred *queue-index qstart probability*

undo wred *queue-index*

View

Ethernet Port View

Parameter

***queue-index*:** index of output queue, in the range of 0~7.

***qstart*:** Start random discarding queue length, if the queue is shorter than the value, no packet will be dropped. Ranging from 1 to 128. The value must be a multiple of 16 KBytes.

***probability*:** discarding probability.

Description

Use the **wred** command to configure WRED parameters. WRED (Weighted Random Early Detection) is a queuing feature used in a network to mitigate the effects of queue congestion.

Use the **undo wred** command to restore the default settings.

By default, the wred function is disabled.

Example

To configure 'start random discarding queue length' of queue 0 is 32kbytes, discarding probability is 50%, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z
[4500]interface Ethernet 1/0/1
[4500-Ethernet1/0/1]wred 0 32 50
[4500-Ethernet1/0/1]
```

Logon User's ACL Control Command

This section describes how to use the logon user's ACL control commands on your Switch 4500.

acl

Syntax

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

undo acl { inbound | **outbound }**

View

User Interface View

Parameter

***acl-number*:** The number identifier of basic and advanced number-based ACLs, ranging from 2000 to 3999.

inbound: Performs ACL control to the users who access the local Switch using TELNET.

outbound: Performs ACL control to the users who access other Switches from the local Switch using TELNET.

Description

Using the **acl** command, you can reference ACL and implement the ACL control to the TELNET users. Using the **undo acl** command, you can remove the control from the TELNET users.

Example

Perform ACL control to the users who access the local Switch using TELNET (basic ACL 2000 has been defined).

```
<4500>system-view
System View: return to User View with Ctrl+Z
[4500]user-interface vty 0 4
[4500-ui-vty0-4]acl 2000 inbound
[4500-ui-vty0-4]
```

ip http acl

Syntax

ip http acl ***acl-number***

undo ip http acl

View

User Interface View

Parameter

***acl-number*:** Specifies a basic ACL with a number in the range of 2000 to 2999.

Description

Use the **ip http acl** command to call an ACL and perform ACL control over the WEB network management users.

Use the **undo ip http acl** command to cancel the ACL control over the WEB network management users.

This command calls numbered basic ACL only.

Example

To perform ACL control over the WEB network management users, enter the following: (Suppose ACL 2020 has been defined.)

```
<4500>system-view
System View: return to User View with Ctrl+Z
[4500]ip http acl 2020
[4500]
```

snmp-agent community

Syntax

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

undo snmp-agent community ***community-name***

View

System View

Parameter

read: Indicates that this community name has the read-only right within the specified view.

write: Indicates that this community name has the read-write right within the specified view.

community-name: Character string of the community name.

mib-view: Set the MIB view name which can be accessed by the community name.

view-name: MIB view name.

acl ***acl-number***: The number identifier of basic number-based ACLs, ranging from 2000 to 2999

Description

Using the **snmp-agent community** command, you can set the community access name, permit the access to the Switch using SNMP, and reference the ACL to perform ACL control to the network management users by acl-number. Using the **undo snmp-agent community** command, you can remove the setting of community access name.

By default, SNMPV1 and SNMPV2C use community name to perform access.

Example

Set the community name as "MyCompany", permit the user to perform read-only access by using this community name, and reference the ACL 2000 to perform ACL control to the network management users (basic ACL 2000 has already been defined).

```
<4500>system-view
System View: return to User View with Ctrl+Z
[4500]snmp-agent community read MyCompany acl 2000
[4500]
```

snmp-agent group

Syntax

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***

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

Parameter

v1: V1 security mode.

v2c: V2c security mode.

v3: V3 security mode.

groupname: Group name, ranging from 1 to 32 bytes.

authentication: If this parameter is added to configuration command, the system will authenticate but not encrypt SNMP data packets.

privacy: Authenticates and encrypts the packets.

read-view: Sets read-only view.

read-view: Read-only view name, ranging from 1 to 32 bytes.

write-view: Sets read-write view.

write-view: Read-write view name, ranging from 1 to 32 bytes.

notify-view: Sets notify view.

notify-view: Notify view name, ranging from 1 to 32 bytes.

acl ***acl-number:*** the number identifier of basic number-based ACLs, ranging from 2000 to 2999

Description

Using the **snmp-agent group** command, you can configure a new SNMP group and reference the ACL to perform ACL control to the network management users by **acl** ***acl-number***. Using the **undo snmp-agent group** command, you can remove a specified SNMP group.

Example

Creates a new SNMP group: MyCompany, and reference the ACL 2001 to perform ACL control to the network management users (basic ACL 2001 has already been defined).

```
<4500>system-view
System View: return to User View with Ctrl+Z
[4500]snmp-agent group v1 MyCompany acl 2001
[4500]
```

snmp-agent usm-user

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***

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

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

View

System View

Parameter

v1: V 1 security mode.

v2c: V 2 security mode.

v3: V 3 security mode.

user-name: The user name, ranging from 1 to 32 bytes.

group-name: The corresponding group name of the user, ranging from 1 to 32 bytes.

authentication-mode: Specifies the security level to "to be authenticated"

md5: Specifies the authentication protocol as HMAC-MD5-96.

sha: Specifies the authentication protocol as HMAC-SHA-96.

auth-password: Authentication password, character string, ranging from 1 to 64 bytes.

privacy: Specifies the security level as encryption.

des56: Specifies the DES encryption protocol.

priv-password: Encryption password, character string, ranging from 1 to 64 bytes.

acl ***acl-number***: The number identifier of basic number-based ACLs, ranging from 2000 to 2999.

local: Local entity user.

engineid: Specifies the engine ID related to the user.

engineid-string: Engine ID character string.

Description

Using the **snmp-agent usm-user** command, you can add a new user to an SNMP group, and reference the ACL to perform ACL control to the network management users by acl acl-number. Using the **undo snmp-agent usm-user** command, you can remove the user from the related SNMP group as well as the configuration of the ACL control of the user.

Example

Add a user "John" to the SNMP group "Mygroup". Specify the security level to "to be authenticated", the authentication protocol to HMAC-MD5-96 and the authentication password to "hello", and reference the ACL 2002 to perform ACL control to the network management users (basic ACL 2002 has already been defined).

```
<4500>system-view
System View: return to User View with Ctrl+Z
```

```
[4500] snmp-agent usm-user v3 John Mygroup authentication-mode md5
hello acl 2002
```

9 USING STACK COMMANDS

This chapter describes how to use the following commands:

Stack Configuration Commands

Stack Commands

This section describes how to use the stack configuration commands on your Switch 4500.

change self-unit

Syntax

change self-unit to { <1-8> | auto-numbering }

View

System View

Parameter

self-unit: Unit ID of the device.

auto-numbering: Changes the unit ID automatically.

Description

Use the **change self-unit** command to change the unit ID of the current Switch. By default, the unit ID of a Switch is set to 1. A unit ID can be set to a value in the range from 1 to the maximum number of devices supported in the stack.

Example

To change the unit ID of the current Switch to 3, enter the following:

```
<4500>system-view
[4500]change self-unit to 3
```

change unit-id

Syntax

change unit-id to < 1-8 >{ < 1-8 > | auto-numbering }

View

System View

Parameter

< 1-8 >: Unit ID of the unit in a stack.

auto-numbering: Change the unit ID automatically.

Description

Use the **change unit-id** command to change the unit ID of a Switch in the stack. By default, the unit ID of a Switch is set to 1. A unit ID can be set to a value in the range from 1 to the maximum number of devices supported in the stack.

- If the modified unit ID does not exist in the stack, the system sets its priority to 5 and saves it in the unit Flash memory.
- If the modified unit is an existing unit, the system will prompt you to confirm if you do want to change the unit ID. If you choose to change, the existing unit ID is replaced and the priority is set to 5. You can then use the **fabric save-unit-id** command to save the modified unit ID into the unit Flash memory and clear the information about the existing unit ID.
- If **auto-numbering** is selected, the system sets the unit ID priority to 10. You can use the **fabric save-unit-id** command to save the modified unit ID into the unit Flash memory and clear the information about the existing unit ID.

Example

To change the unit ID from6 to 4, enter the following:

```
<4500>display ftm topology-database

Total number of UNITs in fabric : 8, My CPU ID : 6
UID CPU-Mac        Prio Fabric-port Chips Mid   Pid A/M
1   00e0-fc00-5502 10   UP/DOWN     2     0/1   3   A
2   00e0-fc03-5502 10   UP/DOWN     2     2/3   3   A
3   00e0-fc04-5502 10   UP/DOWN     2     4/5   3   A
4   00e0-fc05-5502 10   UP/DOWN     2     6/7   3   A
5   00e0-fc06-5502 10   UP/DOWN     2     8/9   3   A
6   00e0-fc07-5502 10   UP/DOWN     2     10/11 3   A
7   00e0-fc04-6502 10   UP/DOWN     2     12/13 3   A
8   00e0-fc01-5502 10   UP/DOWN     2     14/15 5   A

[4500]change unit-id 6 to 4
The unit exists in fabric.
Continue? [Y/N] y

[4500]
%Apr  2 00:48:34:574 2000 4500 FTM/3/DDPFLA:- 6 -Change unitid
successful, un
it 4 saved UnitID(4) in flash!

<4500>display ftm topology-database
Total number of UNITs in fabric : 8, My CPU ID : 4
UID CPU-Mac        Prio Fabric-port Chips Mid   Pid A/M
1   00e0-fc00-5502 10   UP/DOWN     2     0/1   3   A
```

```
2   00e0-fc03-5502 10   UP/DOWN     2     2/3   3   A
3   00e0-fc04-5502 10   UP/DOWN     2     4/5   3   A
6   00e0-fc05-5502 10   UP/DOWN     2     10/11 3   A
5   00e0-fc06-5502 10   UP/DOWN     2     8/9   3   A
4   00e0-fc07-5502 5    UP/DOWN     2     6/7   3   M
7   00e0-fc04-6502 10   UP/DOWN     2     12/13 3   A
8   00e0-fc01-5502 10   UP/DOWN     2     14/15 5   A
```

display ftm

Syntax

display ftm { information | route | topology-database }

View

Any view

Parameter

information: Displays the FTM protocol information.

route: Displays the MAC forwarding table of the fabric.

topology-database: Displays the topology database information of the fabric.

Description

Use the **display ftm information** command to view the FTM protocol information, including DDP status, unit ID, fabric link status, stacking port status and DDp packet statistics.

Use the **display ftm route** command to view the MAC forwarding table of the fabric, which is stored in the CPU.

Use the **display ftm topology-database** command to view the topology database information of the fabric.

Example

To display the FTM protocol information of the Switch, enter the following:

```
[4500]display ftm information
DDP Protocol  : disabled
stacking VLAN : NONE
stacking Auth  : NONE
```

display xrn-fabric

Syntax

display xrn-fabric [port]

View

Any view

Parameter

port: display the stacking port information.

Description

Use the **display xrn-fabric** command to view the information of the entire stack, including unit ID, unit name, operation mode. If the stack information is

displayed on the console port of a device, an asterisk (*) next to the unit ID indicates the current device.

Example

To display fabric information on the console port of unit 1, enter the following:

```
[4500]display xrn-fabric
Fabric name is 4500 , system mode is L3.
Fabric authentication: no authentication, number of units in stack:
1.
Unit Name                                  Unit ID
First                                      1(*)
```

fabric save-unit-id

Syntax

fabric save-unit-id
undo fabric save-unit-id

View

User View

Parameter

None

Description

Use the **fabric save-unit-id** command to save the unit ID of all units in a stack, into the unit Flash memory and set the priority to 5.

Use the **undo fabric save-unit-id** command to restore the unit ID of the units in a stack.

Example

To save the unit ID of all units in a stack to the unit Flash memory, enter the following:

```
[4500]display ftm topology-database
Total number of UNITs in fabric : 8, My CPU ID : 4
UID CPU-Mac        Prio stacking-port Chips Mid   Pid A/M
1   00e0-fc00-5502 10   UP/DOWN     2     0/1   3   A
4   00e0-fc03-5502 10   UP/DOWN     2     6/7   3   A
3   00e0-fc04-5502 10   UP/DOWN     2     4/5   3   A
6   00e0-fc05-5502 10   UP/DOWN     2     10/11 3   A
5   00e0-fc06-5502 10   UP/DOWN     2     8/9   3   A
2   00e0-fc07-5502 10   UP/DOWN     2     2/3   3   A
7   00e0-fc04-6502 10   UP/DOWN     2     12/13 3   A
8   00e0-fc01-5502 10   UP/DOWN     2     14/15 5   A
[4500]quit

<4500>fabric save-unit-id
 The unit ID will be saved to the device.
 Are you sure? [Y/N] y
%Apr  2 02:13:44:413 2000 3200 FTM/3/DDPFLA:- 4 -Save self unitid,
unit 4 sav
ed UnitID(4) in flash!
 Unit 1 saved unit ID successfully.
 Unit 2 saved unit ID successfully.
```

```
 Unit 3 saved unit ID successfully.
 Unit 4 saved unit ID successfully.
 Unit 5 saved unit ID successfully.
 Unit 6 saved unit ID successfully.
 Unit 7 saved unit ID successfully.
 Unit 8 saved unit ID successfully.

<4500>display ftm topology-database
Total number of UNITs in fabric : 8, My CPU ID : 4
UID CPU-Mac         Prio stacking-port Chips Mid   Pid A/M
1   00e0-fc00-5502 5    UP/DOWN     2     0/1   3   M
4   00e0-fc03-5502 5    UP/DOWN     2     6/7   3   M
3   00e0-fc04-5502 5    UP/DOWN     2     4/5   3   M
6   00e0-fc05-5502 5    UP/DOWN     2     10/11 3   M
5   00e0-fc06-5502 5    UP/DOWN     2     8/9   3   M
2   00e0-fc07-5502 5    UP/DOWN     2     2/3   3   M
7   00e0-fc04-6502 5    UP/DOWN     2     12/13 3   M
8   00e0-fc01-5502 5    UP/DOWN     2     14/15 5   M
```

fabric-port enable

Syntax

fabric-port { *interface-type interface-num* } enable

undo fabric-port { *interface-type interface-num* } enable

View

System View

Parameter

interface-type interface-num Displays the interface type and number

Description

Use the **fabric-port enable** command to specify the Fabric port of the Switch.

Use the **undo fabric-port enable** command to cancel the Fabric port of the Switch.

Example

To set GigabitEthernet1/0/51 to stacking port mode, enter the following:

```
[4500]fabric-port gigabitEthernet1/0/51 enable
```

ftm stacking-vlan

Syntax

ftm stacking-vlan *vlan-id*

undo ftm stacking-vlan

View

System View

Parameter

vlan-id: Specifies the VLAN used for stacking. By default, the stacking VLAN is VLAN 4093.

Description

Use the **ftm stacking-vlan** command to specify the stacking VLAN of the Switch.

Use the **undo ftm stacking-vlan** command to set the stacking VLAN of the Switch to its default value.

You should specify the stacking VLAN before the stack is established.

Example

Set VLAN 2 as stacking VLAN:

```
[4500]ftm stacking-vlan 2
```

xrn-fabric authentication-mode

Syntax

xrn-fabric authentication-mode { simple *password* | md5 *key* }

undo xrn-fabric authentication-mode

View

System View

Parameter

***password*:** Password, in the range of 1 to 16 characters.

***key*:** Key word, in the range of 1 to 16 characters.

Description

Use the **xrn-fabric authentication-mode** command to configure or delete the authentication mode of the fabric.

By default, no authentication mode is configured on the stack.

CAUTION: *All units must have the same stack authentication settings in order to form a stack of units.*

Example

To set the authentication mode of the stack to simple, with the password "hello", enter the following:

```
[4500]xrn-fabric authentication-mode simple hello
```

set unit name

Syntax

set unit *unit-id* name *unit-name*

View

System View

Parameter

***unit-id*:** Unit ID of a device.

***unit-name*:** Unit name of a device. It is a string comprising 0 to 64 characters.

Description

You can use this command to set a name for a device.

Example

To set the name "hello" for the device with unit ID 1, enter the following:

```
<4500>display xrn-fabric

Fabric name(HostName): 4500

Fabric authentication: md5, Fabric mode: L3, number of units in
stack: 2

Unit Name     Unit ID
Hello         1
Second        2(*)
```

sysname

Syntax

sysname ***sysname***

undo sysname

View

System View

Parameter

***sysname*:** A string comprising 1 to 30 characters. By default, the stack name of Ethernet Switch is 4500.

Description

Use the **sysname** command to change the name of the stack. The modification will affect the prompt character in the command line interface. For example, if the stack name of the Switch is 4500, the prompt character in user view is <4500>.

Use the **undo sysname** command to restore the default fabric name.

Example

To change the fabric name of the device to "hello", enter the following:

```
<4500>display xrn-fabric

Fabric name(HostName): 4500

Fabric authentication: md5 Fabric mode: L3, number of units in stack:
2

Unit Name     Unit ID
First           1
Second          (2)*

[4500]sysname hello
[hello]display xrn-fabric
Fabric name(HostName): hello
Fabric authentication md5, Fabric mode :L3, number of units in stack:
2.
```

```
Unit Name     Unit ID
First           1
Second          2 (*)
```

10 USING RSTP COMMANDS

This chapter describes how to use the following commands:

RSTP Configuration Commands

RSTP Configuration Commands

This section describes how to use the Rapid Spanning Tree Protocol (RSTP) configuration commands on your Switch.

display stp

Syntax

display stp [interface *interface_list*]

display stp brief

View

All views

Parameter

interface *interface_list*: Specifies the Ethernet port list, including multiple Ethernet ports. Expressed as ***interface _list={ { interface_type interface_num*** | ***interface_name } [*** **to** ***{ interface_type interface_num*** | ***interface_name }] }&<1-10>***.

For details about ***interface_type, interface_num*** and ***interface_name***, refer to the **port** command in this guide.

***&<1-10>*:** Indicates the preceding parameter can be input up to 10 times.

Description

Use the **display stp** command to view the status information of the current RSTP.

Use the **display stp brief** command to view summary information of the STP state of the Switch.

Related command: **reset stp**.

Example

To display the RSTP status information for Ethernet1/0/2, enter the following:

```
<4500>display stp interface Ethernet1/0/2
Protocol mode: IEEE RSTP
 The bridge ID (Pri.MAC): 32768.00e0-fc00-3900
 The bridge times: Hello Time 2 sec, Max Age 20 sec, Forward Delay 15
sec
 Root bridge ID(Pri.MAC): 32768.00e0-fc00-3900
 Root path cost: 0
 Bridge bpdu-protection: disabled
 Default path cost standard is dot1t
 Timeout factor: 3

 Port 2 (Ethernet1/0/2) of bridge is DOWN
   Port spanning tree protocol: enabled
   Port role: Disabled Port
   Port path cost: 2000000
   Port priority: 128
   Designated bridge ID(Pri.MAC): 32768.00e0-fc00-3900
   The Port is a non-edged port
   Connected to a non-point-to-point LAN segment
   Maximum transmission limit is 3  Packets / hello time
```

```
Times: Hello Time 2 sec,    Max Age 20 sec
       Forward Delay 15 sec, Message Age 0
BPDU sent:     0
       TCN: 0, RST: 0, Config BPDU: 0
BPDU received: 0
       TCN: 0, RST: 0, Config BPDU: 0
```

Table 27 Display information

Field	Description
Protocol mode	Current Switch is executing RSTP.
The bridge ID (Pri.MAC): 32768.00e0-fc00-3900 The bridge times: Hello Time 2 sec, Max Age 20 sec, Forward Delay 15 sec Root bridge ID(Pri.MAC): 32768.00e0-fc00-3900 Root path cost: 0 Bridge bpdu-protection: disabled Default path cost standard is dot1t Timeout factor: 3	The RSTP configuration of the Switch, including priority and MAC address of local bridge, Configured time parameter (Hello Time, Max Age, Forward Delay), priority and MAC address of root bridge, the path cost from this Switch to the root path cost mode, timeout time.
Port 2 (Ethernet1/0/2) of bridge is DOWN Port spanning tree protocol: enabled Port role: Disabled Port Port path cost: 200000 Port priority: 128 Designated bridge ID(Pri.MAC): 32768.00e0-fc00-3900 The Port is a non-edged port Connected to a non-point-to-point LAN segment Maximum transmission limit is 3 Packets / hello time Times: Hello Time 2 sec, Max Age 20 sec Forward Delay 15 sec, Message Age 0 BPDU sent: 0 TCN: 0, RST: 0, Config BPDU: 0 BPDU received: 0 TCN: 0, RST: 0, Config BPDU: 0	The RSTP configuration of port 2, including the port's status is down, the port RSTP is enabled, this port is Disabled Port, the cost to root of this port , the priority of this port, the priority and MAC address of Designated bridge, this port is configured as a non-edge port, the link of this port is non-point-to-point, Maximum transmission limit is 3 BPDUs per hello time, configured RSTP time parameters(Hello Time, Max Age, Forward Delay, Message Age), the statistics of BPDU (TCN specifies the number of topology-change-notify datagram, RST specifies the number of RSTP datagram, Config BPDU specifies the number of STP datagram)

reset stp

Syntax

`reset stp [ interface` ***`interface_list`*** **`]`**

View

User view

Parameter

interface *interface_list*: Specifies the Ethernet port list, including multiple Ethernet ports. Expressed as `interface _list = { { interface_type interface_num | interface_name } [ to { interface_type interface_num | interface_name } ] }&<1-10>`.

For details about ***interface_type***, ***interface_num*** and ***interface_name***, refer to the **port** command in this guide.

***&<1-10>*:** Indicates the preceding parameter can be input up to 10 times.

Description

Use the **reset stp** command to reset the statistics information about Rapid Spanning Tree Protocol (RSTP).

This command can be used to clear the statistics information about a specified port. If no port is specified, the statistics information of all the ports of the device will be cleared.

Related command: **display stp**.

Example

To clear the statistics information about Ethernet1/0/1 through Ethernet1/0/3, enter the following:

```
<4500>reset stp interface Ethernet1/0/1 to Ethernet1/0/3
```

stp

Syntax

stp { enable | disable }

undo stp

View

Ethernet Port View

Parameter

enable: Enables RSTP on a device or a port.

disable: Disables RSTP on a device or a port.

Description

Use the **stp enable** command to enable RSTP on a device or port.

Use the **stp disable** command to disable RSTP on a device or port.

Use the **undo stp** command to disable RSTP on a device.

By default, RSTP is enabled on the Switch and all ports.

If the parameters of RSTP have not been set for the device or the ports before RSTP is enabled on the device, they will take the default values. Before or after RSTP is enabled, you can use the configuration command to set RSTP parameters

for the device and ports. This command enables/disables RSTP on a device in system view and enables/disables RSTP on a port in Ethernet Port View.

Related command: **stp mode**.

Example

To enable RSTP on a Switch, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]stp enable
```

To disable RSTP on Ethernet1/0/1, enter the following:

```
[4500]interface Ethernet1/0/1
[4500-Ethernet1/0/1]stp disable
```

stp bpdu-protection

Syntax

stp bpdu-protection

undo stp bpdu-protection

View

System view

Parameter

None

Description

Use the **stp bpdu-protection** command to enable BPDU protection on a Switch.

Use the **undo stp bpdu-protection** command to resume the default status of BPDU protection function.

By default, BPDU protection is not enabled.

For an access layer device, its ports are generally directly connected to a user terminal (such as a PC) or file server, and configured as an edge port to implement fast transition. When such a port receives BPDU packets, the system will set it to a non-edge port and recalculate the spanning tree, which will cause network topology flapping. In normal circumstances, these ports should not receive any BPDU packets. However, someone may forge BPDU to maliciously attack the Switch and cause network flapping.

RSTP provides the BPDU protection function against such an attack. After the BPDU protection function is enabled on a Switch, the system will disable an edge port that has received BPDUs and notify the network manager about it. The disabled port can only be re-enabled by the network manager.

Example

To enable BPDU protection function on a Switch, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
```

```
[4500]stp bpdu-protection
```

stp cost

Syntax

stp cost *cost*

undo stp cost

View

Ethernet Port View

Parameter

***cost*:** Specifies the path cost, ranging from 1 to 2000000.

Description

Use the **stp cost** command to configure the path cost on a spanning tree for the current Ethernet port.

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

By default, the bridge gets the path cost directly through the speed of the link connected to the port.

The path cost of an Ethernet port is related to the link speed. You can refer to the following table. RSTP will check the link speed of the port and get the path cost directly. It is recommended to set the cost to the default value and let RSTP query the path cost of the port.

Table 28 Path cost for ports at different link speeds

Link Speed	IEEE Recommended Value	IEEE Recommended Range	Switch Range
10Mbps	2000000	20000 to 20000000	1 to 2000000
100Mbps	200000	20000 to 2000000	1 to 2000000
1Gbps	20000	2000 to 200000	1 to 2000000
10Gbps	2000	200 to 20000	1 to 2000000

Example

To configure the path cost of Ethernet1/0/1 to 200000, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface Ethernet1/0/1
[4500-Ethernet1/0/1]stp cost 200000
```

stp edged-port

Syntax

stp edged-port { enable | disable }

undo stp edged-port

View

Ethernet Port View

Parameter

enable: Sets the current Ethernet port as an edge port.

disable: Sets the current Ethernet port as a non-edge port.

Description

Use the **stp edged-port enable** command to configure the current port as an edge port.

Use the **stp edged-port disable** command to configure the current port as a non-edge port.

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

By default, all the Ethernet ports of the bridge are configured as non-edge ports.

If the current Ethernet port is connected to other Switch, you can use the **stp edged-port disable** or **undo stp edged-port** command to specify it as a non-edge port. The stp edged-port enable command can be used to configure the current Ethernet port as an edge port. All the Ethernet ports have been set to non-edge ports by default. You can configure the Ethernet ports directly connected to the user terminals as edge ports, so that they can transition to forwarding state quickly.

Related command: **stp point-to-point**.

Example

To set Ethernet1/0/1 as a non-edge port, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface Ethernet1/0/1
[4500-Ethernet1/0/1]stp edged-port disable
```

stp loop-protection

Syntax

stp loop-protection

undo stp loop-protection

View

Ethernet Port View

Parameter

none

Description

Use the **stp loop-protection** command to enable loop protection function.

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

By default, the loop protection function is not enabled.

Example

To enable loop protection function in Ethernet1/0/1, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface Ethernet1/0/1
[4500-Ethernet1/0/1]stp loop-protection
```

stp mcheck

Syntax

stp mcheck

View

System View

Parameter

None

Description

If the network is unstable, even when the bridge running STP on the segment is removed, the corresponding port will still work in the STP compatible mode.

Use the **stp mcheck** command to force the port to work in RSTP mode.

If there is any bridge running STP on the segment connected to the current Ethernet port, the port will Switch to run RSTP in STP compatible mode. If the network is rather stable, even when the bridge running STP on the segment is removed, the corresponding port will still work in the STP compatible mode. In this case, you can use this command to force the port to work in RSTP mode. In RSTP mode, when the port receives an STP packet, it will transition to the STP compatible mode.

The configuration can only be performed when the bridge runs in RSTP mode. If the bridge is configured to work in STP compatible mode, the command will not make any sense.

Related command: **stp mode**.

Example

To set the port Ethernet1/0/1 to work in RSTP mode, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface Ethernet1/0/1
[4500-Ethernet1/0/1]stp mcheck
```

stp mode

Syntax

stp mode { stp | rstp }

undo stp mode

View

System view

Parameter

stp: Specifies to run Spanning Tree in STP compatible mode.

rstp: Specifies to run Spanning Tree in RSTP mode.

Description

Use the **stp mode** command to configure Spanning Tree's running mode.

Use the **undo stp mode** command to restore the default Spanning Tree's running mode.

By default, the value is rstp.

This command can be used for specifying the current Ethernet Switch to run the Spanning Tree in RSTP mode or in STP compatible mode.

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

Example

To set Spanning Tree to work in STP compatible mode, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]stp mode stp
```

stp pathcost-standard

Syntax

stp pathcost-standard { dot1d-1998 | dot1t }

undo stp pathcost-standard

View

System view

Parameter

dot1d-1998: The Switch calculates the default Path Cost of a port by the IEEE 802.1D-1998 standard.

dot1t: The Switch calculates the default Path Cost of a port by the IEEE 802.1t standard.

Description

Use the **stp pathcost-standard** command to specify the standard to be used by the Switch in calculating the default Path Cost.

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

By default, the Switch calculates the default Path Cost of a port by the IEEE 802.1t standard.

Example

To configure the Switch to calculate the default Path Cost of a port by the IEEE 802.1D-1998 standard, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]stp pathcost-standard dot1d-1998
```

To configure the Switch to calculate the default Path Cost of a port by the IEEE 802.1t standard, enter the following:

```
[4500]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

Parameter

force-true: Indicates that the link to the current Ethernet port is a point-to-point link.

force-false: Indicates that the link to the current Ethernet port is not a point-to-point link.

auto: Specifies to automatically check if the link to the Ethernet port is a point-to-point link or not.

Description

Use the **stp point-to-point** command to configure the state of the link to the current Ethernet port as a point-to-point link or not a point-to-point link.

Use the **undo stp point-to-point** command to restore the default status of the link, that is, RSTP is responsible for checking whether the link to the current Ethernet port is a point-to-point link or not.

By default, the value is auto.

Example

To indicate that the link to Ethernet1/0/1 is a point-to-point link, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface Ethernet1/0/1
[4500-Ethernet1/0/1]stp point-to-point force-true
```

stp port priority

Syntax

stp port priority ***port-priority***

undo stp port priority

View

Ethernet Port View

Parameter

***port-priority*:** Specifies the priority of the port, ranging from 0 to 240. The values are not consecutive integers. Step length is 16. By default, the value is 128.

Description

Use the **stp port priority** command to configure the priority of the current Ethernet port.

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

The priority value shall be a multiple of 16, such as 0, 16, 32, 48 etc. The smaller value represents the higher priority. A port with higher priority (lower numerical value) is more likely to be a root port.

Example

To set the priority of Ethernet1/0/1 to 64, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface Ethernet1/0/1
[4500-Ethernet1/0/1]stp port priority 64
```

stp priority

Syntax

stp priority *bridge-priority*

undo stp priority

View

System View

Parameter

***bridge-priority*:** Specifies the priority of a Switch, ranging from 0 to 61440. The values are not consecutive integers. The step length is 4096. By default, the value is 32768.

Description

Use the **stp priority** command to configure the bridge priority of the Switch.

Using **undo stp priority** command, you can restore the default bridge priority of the Switch.

The priority value shall be a multiple of 4096, such as 0, 4096, 8192 etc. The smaller value represents the higher priority. A Switch with higher priority is more likely to be a root bridge.

Example

To set the priority of the Switch to 4096, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]stp priority 4096
```

stp root primary

Syntax

stp root primary

undo stp root

View

System View

Parameter

None

Description

Use the **stp root primary** command to configure the current Switch as the primary root of a spanning tree.

Use the **undo stp root** command to cancel the current Switch for primary root of a spanning tree.

By default, the Switch is not a primary root.

You can designate a primary root for the spanning tree without caring about the priority configuration of the Switch.

CAUTION: *In a switching network, you can configure no more than one primary root for a spanning tree but you can configure one or more secondary roots for it. Remember not to designate more than one primary root in a spanning tree; otherwise, the switching behavior will be unpredictable.*

After a Switch is configured as a primary root bridge or secondary root bridge, you can not modify the bridge priority of the Switch.

Example

To designate the current Switch as the primary root of a spanning tree, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]stp root primary
```

stp root secondary

Syntax

stp root secondary

undo stp root

View

System view

Parameter

None

Description

Use the **stp root secondary** command to configure the current Switch as a secondary root of a specified spanning tree.

Use the **undo stp root** command to cancel the designation of the current Switch for a secondary root of a specified spanning tree.

By default, a Switch is not a secondary root.

You can designate one or more secondary roots for a spanning tree. When the primary root fails or is powered off, a secondary root can take its place. If more than one secondary root exists, the one with the smallest MAC address will become the primary root of the specified spanning tree.

You can configure no more than one primary root for a spanning tree but you can configure one or more secondary roots for it. You cannot change the bridge priority of a Switch if you configure it as a secondary root of a spanning tree.

Example

To designate the Switch as a secondary root of the STP, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]stp root secondary
```

stp root-protection

Syntax

stp root-protection

undo stp root-protection

View

Ethernet Port View

Parameter

None

Description

Use the **stp root-protection** command to enable Root protection function on a Switch.

Use the **undo stp root-protection** command to restore the default status of Root protection function.

By default, root protection is not enabled.

Following incorrect configuration or malicious attack, a legal root of the network may receive a BPDU with higher priority and lose its status as root, which causes problems with the network topology. Such problems may pull the higher-speed traffic to lower-speed links and cause network congestion.

To avoid this problem, RSTP provides Root protection function. After being configured with Root protection, a port always stays as a designated port. Once this port receives a BPDU with higher priority, it turns to listening status and will

not forward any packets (as if the link to it is disconnected). It will resume normal status if it receives no BPDU with higher-priority for a period of time.

Example

To enable Root protection function on Ethernet1/0/1 of the Switch, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface Ethernet1/0/1
[4500-Ethernet1/0/1]stp root-protection
```

stp timeout-factor

Syntax

stp timeout-factor ***number***

undo stp timeout-factor

View

System View

Parameter

***number*:** Specifies the multiple of hello time, ranging from 3 to 7.

Description

Use the **stp timeout-factor** command to configure the multiple of hello time for the Switch.

Use the **undo stp timeout-factor** command to restore the default multiple value.

By default, the multiple is 3.

The Ethernet Switch transmits RSTP packets every hello time seconds. By default, if the Switch does not receive RSTP packets from the upstream Switch for 3 x hello time seconds, the Switch will decide the upstream Switch is dead and will recalculate the topology of the network. In a congested network, a system administrator may want to increase the timeout interval to prevent an unnecessary network topology change. This can be accomplished by using the timeout-factor command to set the multiplier to the desired value. The higher the multiplier the greater the timeout interval. It is recommended to set 5, 6 or 7 as the value of multiple in the steady network.

Example

To set the multiple value of hello time to 7, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]stp timeout-factor 7
```

stp timer forward-delay

Syntax

stp timer forward-delay ***centiseconds***

undo stp timer forward-delay

View

System View

Parameter

***centiseconds*:** Specifies the time of forward delay in centiseconds, ranging from 400 to 3000. By default, the value is 1500 centiseconds.

Description

Use the **stp timer forward-delay** command to configure the time of forward delay for the Switch.

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

The value of forward delay is related to the "diameter" of the switching network. The more extensive the switching network is, the longer the forward delay should be set. You can use this command to modify the value of forward delay. The default value, 1500, is recommended.

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

Example

To set the forward delay of the device to 2000 centiseconds, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]stp timer forward-delay 2000
```

stp timer hello

Syntax

stp timer hello centiseconds

undo stp timer hello

View

System View

Parameter

***centiseconds*:** Specifies the value of hello time in centiseconds, ranging from 100 to 1000. By default, the value is 200 centiseconds.

Description

Use the **stp timer hello** command to configure hello time of the Switch.

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

The Ethernet Switch transmits RSTP packets every hello time seconds. A longer hello time can ease the CPU load of the Switch, but it will also affect the performances of RSTP in how rapidly it responds to changes. The **stp timer hello** command can be used to modify the value of hello time. The default value is recommended.

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

Example

To set the hello time of the Switch to 300 centiseconds, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]stp timer hello 300
```

stp timer max-age

Syntax

stp timer max-age ***centiseconds***

undo stp timer max-age

View

System View

Parameter

***centiseconds*:** Specifies the maximum age in centiseconds, ranging from 600 to 4000. By default, the value is 2000 centiseconds.

Description

Use the **stp timer max-age** command to configure the Max Age of the Switch.

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

Maximum age is used for judging if an RSTP packet is outdated. If the value is set too small, the spanning tree will be computed too frequently because the network congestion may be considered as a link failure. However, if the value is set too large, the link failure may not be discovered in time. Maximum age is related to the network "diameter", or complexity of the switched network. The default value, 2000, is recommended.

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

Example

To set the Max Age of the Switch to 1000 centiseconds, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]stp timer max-age 1000
```

stp transmit-limit

Syntax

stp transmit-limit ***packetnum***

undo stp transmit-limit

View

Ethernet Port View

Parameter

***packetnum*:** The maximum number of STP packets a port can send within one hello time. It ranges from 1 to 255 and defaults to 3.

Description

Use the **stp transmit-limit** command to set the maximum number of STP packets the current port can send within one hello time.

Use the **undo stp transmit-limit** command to restore the default value.

The larger the value of ***packetnum*** is, the larger the transmission rate is. However, more Switch resources will be used.

Example

To set the ***packetnum*** parameter of Ethernet1/0/1 to 5, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]interface Ethernet1/0/1
[4500-Ethernet1/0/1]stp transmit-limit 5
```

11 USING AAA AND RADIUS COMMANDS

This chapter describes how to use the following commands:

802.1x Configuration Commands

- display dot1x
- dot1x
- dot1x authentication-method
- dot1x dhcp-launch
- dot1x max-user
- dot1x port-control
- dot1x port-method
- dot1x quiet-period
- dot1x retry
- dot1x supp-proxy-check
- dot1x timer
- reset dot1x statistics

Centralized MAC Address Authentication Configuration Commands

- debugging mac-authentication event
- display mac-authentication
- mac-authentication
- mac-authentication authmode
- mac-authentication authpassword
- mac-authentication authusername
- mac-authentication domain
- mac-authentication timer

AAA Configuration Commands

- access-limit
- attribute
- cut connection
- display connection
- display domain
- display local-user

- domain
- idle-cut
- level
- local-user
- local-user password-display-mode
- messenger
- password
- radius-scheme
- scheme
- self-service-url
- service-type
- state

RADIUS Protocol Configuration Commands

- accounting optional
- data-flow-format
- display local-server statistics
- display radius
- display radius statistics
- display stop-accounting-buffer
- key
- local-server
- nas-ip
- primary accounting
- primary authentication
- radius nas-ip
- radius scheme
- reset radius statistics
- reset stop-accounting-buffer
- retry
- retry realtime-accounting
- retry stop-accounting
- secondary accounting
- secondary authentication
- server-type
- state
- stop-accounting-buffer enable
- timer
- timer quiet

- timer realtime-accounting
- timer response-timeout
- user-name-format

802.1x Configuration Commands

This section describes how to use the 802.1x configuration commands on your Switch 4500.

display dot1x

Syntax

display dot1x [sessions | statistics [interface *interface-list*]]

View

All views

Parameter

interface: Displays the 802.1x information on the specified interface.

sessions: Displays the session connection information of 802.1x.

statistics: Displays the relevant statistics information of 802.1x.

interface-list*:** Ethernet interface list including several Ethernet interfaces, expressed in the format ***interface-list* = { *interface-num* [to *interface-num*] } & < 1-10 >**. *interface-num* specifies a single Ethernet interface in the format ***interface-num* = { *interface-type interface-num* | *interface-name* }**, where ***interface-type specifies the interface type, ***interface-num*** specifies the interface number and ***interface-name*** specifies the interface name. For the respective meanings and value ranges, refer to "Parameter" in "Using Port Commands".

Description

Use the **display dot1x** command to view the relevant information of 802.1x, including configuration information, running state (session connection information) and relevant statistics information.

By default, all the relevant 802.1x information about each interface will be displayed.

This command can be used to display the following information on the specified interface: 802.1x configuration, state or statistics. If no port is specified when executing this command, the system will display all 802.1x related information. For example, 802.1x configuration of all ports, 802.1x session connection information, and 802.1x data statistical information. The output information of this command can help the user to verify the current 802.1x configurations so as to troubleshoot 802.1x.

Related commands: **reset dot1x statistics**, **dot1x**, **dot1x retry**, **dot1x max-user**, **dot1x port-control**, **dot1x port-method**, **dot1x timer**.

Example

Display the configuration information of 802.1x.

```
<4500>display dot1x
Equipment 802.1X protocol is enabled
 DHCP-launch is disabled
 EAP-relay is enabled
 Proxy trap checker is disabled
 Proxy logoff checker is disabled
```

```
 Configuration: Transmit Period 30 s,  Handshake Period 15 s
                Quiet Period 60 s,  Quiet Period Timer is disabled
                Supp Timeout 30 s,  Server Timeout 100 s
                The Max-Req 3

 Total maximum 802.1x user resource number is 1024

 Total current used 802.1x resource number is 0

 Ethernet1/0/1 is link-up
   802.1X protocol is disabled
   Proxy trap checker is disabled
   Proxy logoff checker is disabled
   The port is a(n) authenticator
   Authentication Mode is Auto
   Port Control Type is Mac-based
   Max number of on-line users is 256
… (Omitted)
```

dot1x

Syntax

dot1x [interface *interface-list*]

undo dot1x [interface *interface-list*]

View

Ethernet Port View

Parameter

interface *interface-list:* Ethernet port list including several Ethernet ports. ***interface-list* = { *interface-num* [to *interface-num*] } & < 1-10 >.** ***interface-num*** specifies a single Ethernet port in the format ***interface-num* = { *interface-type interface-num* | *interface-name* }**, where ***interface-type*** specifies the port type, ***interface-num*** specifies the port number and ***interface-name*** specifies the port name. For the respective meanings and value ranges, read the Parameter of the Port Configuration section.

Description

Use the **dot1x** command to enable 802.1x on the specified port or globally, (that is on the current device). Use the **undo dot1x** command to disable the 802.1x on the specified port or globally.

By default, 802.1x is disabled on all the ports and globally on the device.

This command is used to enable the 802.1x on the current device or on the specified port. When it is used in System View, if the parameter ***ports-list*** is not specified, 802.1x will be globally enabled. If the parameter ***ports-list*** is specified, 802.1x will be enabled on the specified port. When this command is used in Ethernet Port View, the parameter interface-*list* cannot be entered and 802.1x can only be enabled on the current port.

The configuration command can be used to configure the global or port 802.1x performance parameters before or after 802.1x is enabled. Before 802.1x is

enabled globally, if the parameters are not configured globally or for a specified port, they will maintain the default values.

After the global 802.1x performance is enabled, only when port 802.1x performance is enabled will the configuration of 802.1x become effective on the port.

Related commands: **display dot1x**.

Example

To enable 802.1x on Ethernet 1/0/1, enter the following.

```
<4500>system-view
System View: return to User View with Ctrl-Z
[4500]dot1x interface ethernet 1/0/1
```

To enable 802.1x globally, enter the following.

```
[4500]dot1x
```

dot1x authentication-method

Syntax

dot1x authentication-method { chap | pap | eap }

undo dot1x authentication-method

View

System View

Parameter

Chap: Use CHAP authentication method.

Pap: Use PAP authentication method.

eap: Use EAP authentication method.

Description

Use the **dot1x authentication-method** command to configure the authentication method for the 802.1x user. Use the **undo dot1x authentication-method** command to restore the default authentication method of the 802.1x user.

By default, CHAP authentication is used for 802.1x user authentication.

Password Authentication Protocol (PAP) is a kind of authentication protocol with two handshakes. It sends the password in the form of simple text.

Challenge Handshake Authentication Protocol (CHAP) is a kind of authentication protocol with three handshakes. It only transmits the username, not the password. CHAP is more secure and reliable.

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.

To use PAP, CHAP or EAP authentication, RADIUS server should support PAP, CHAP or EAP authentication respectively.

Related command: **display dot1x**.

Example

Configure 802.1x user to use PAP authentication

```
<4500>system-view
System View: return to User View with Ctrl-Z
[4500]dot1x authentication-method pap
```

dot1x dhcp-launch

Syntax

dot1x dhcp-launch

undo dot1x dhcp-launch

View

System View

Parameter

None

Description

Use the **dot1x dhcp-launch** command to set 802.1x to prevent the Switch from triggering user ID authentication for users who configure static IP addresses in a DHCP environment. Use the **undo dot1x dhcp-launch** command to allow the Switch to trigger ID authentication.

By default, the Switch can trigger user ID authentication for users who configure static IP addresses in a DHCP environment.

Related command: **dot1x**.

Example

Prevent the Switch from triggering the authentication ID for users who configure static IP addresses in a DHCP environment.

```
<4500>system-view
System View: return to User View with Ctrl-Z
[4500]dot1x dhcp-launch
```

dot1x max-user

Syntax

dot1x max-user *user-number* [interface *interface-list*]

undo dot1x max-user [interface *interface-list*]

View

Ethernet Port View

Parameter

user-number: Specifies the limit to the amount of supplicants on the port, ranging from 1 to 1024.

By default, the maximum user number is 1024.

interface *interface-list:* Ethernet interface list including several Ethernet interfaces, expressed in the format ***interface-list* = { *interface-num* [to *interface-num*] } & < 1-10 >**. ***interface-num*** specifies a single Ethernet interface in the format ***interface-num* = { *interface-type interface-num* | *interface-name* }**, where *interface-type* specifies the interface type, ***interface-num*** specifies the interface number and ***interface-name*** specifies the interface name. For the respective meanings and value ranges, see the parameters in the Port Command chapter.

Description

Use the **dot1x max-user** command to configure a limit to the amount of supplicants on the specified interface using 802.1x. Use the **undo dot1x max-user** command to restore the default value.

This command is used for setting a limit to the amount of supplicants that 802.1x can hold on the specified interface. This command takes effect on the interface specified by the parameter ***interface-list*** when executed in System View. It takes effect on all the interfaces when no interface is specified. The parameter ***interface-list*** cannot be entered when the command is executed in Ethernet Port View and it takes effect only on the current interface.

Related command: **display dot1x**.

Example

Configure the interface Ethernet 1/0/2 to hold no more than 32 802.1x users.

```
<4500>system-view
System View: return to User View with Ctrl-Z
[4500]dot1x max-user 32 interface ethernet 1/0/2
```

dot1x port-control

Syntax

dot1x port-control { auto | authorized-force | unauthorized-force-} [interface *interface-list*]

undo dot1x port-control [interface *interface-list*]

View

Ethernet Port View

Parameter

auto: Automatic identification mode, configuring the initial state of the interface as unauthorized. The user is only allowed to receive or transmit EAPoL packets but not to access the network resources. If the user passes the authentication flow, the interface will Switch over to the authorized state and then the user is allowed to access the network resources. This is the most common case.

authorized-force: Forced authorized mode, configuring the interface to always stay in authorized state and the user is allowed to access the network resources without authentication/authorization.

unauthorized-force: Forced unauthorized mode, configuring the interface to always stay in non-authorized mode and the user is not allowed to access the network resources.

interface *interface-list:* Ethernet interface list including several Ethernet interfaces, expressed in the format ***interface-list* = { *interface-num* [to *interface-num*] } & < 1-10 >**. ***interface-num*** specifies a single Ethernet interface in the format ***interface-num* = { *interface-type interface-num* | *interface-name* }**, where ***interface-type*** specifies the interface type, ***interface-num*** specifies the interface number and *interface-name* specifies the interface name. For the respective meanings and value ranges, see the parameters of the Port Command chapter.

Description

Use the **dot1x port-control** command to configure the mode for 802.1x to perform access control on the specified interface. Use the **undo dot1x port-control** command to restore the default access control mode.

By default, the value is ***auto***.

This command is used to set the mode, or the interface state, for 802.1x to perform access control on the specified interface. This command has an effect on the interface specified by the parameter ***interface-list*** when executed in System View. It has an effect on all the interfaces when no interface is specified. The parameter ***interface-list*** cannot be entered when the command is executed in Ethernet Port View and it has an effect only on the current interface.

Related command: **display dot1x**.

Example

To configure the interface Ethernet 1/0/2 to be in force-unauthorized state, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl-Z
[4500]dot1x port-control force-unauthorized interface ethernet 1/0/2
```

dot1x port-method

Syntax

dot1x port-method { macbased | portbased } [interface *interface-list*]

undo dot1x port-method [interface *interface-list*]

View

Ethernet Port View

Parameter

macbased: Configures the 802.1x authentication system to perform authentication on the supplicant based on MAC address.

portbased: Configures the 802.1x authentication system to perform authentication on the supplicant based on interface number.

interface *interface-list:* Ethernet interface list including several Ethernet interfaces, expressed in the format ***interface-list* = { *interface-num* [to *interface-num*] } & < 1-10 >**. ***interface-num*** specifies a single Ethernet interface in the format ***interface-num* = { *interface-type interface-num* | *interface-name* }**, where *interface-type* specifies the interface type, ***interface-num*** specifies the interface number and ***interface-name*** specifies the interface name. For the respective meanings and value ranges, see the parameters in the Port Command chapter.

Description

Use the **dot1x port-method** command to configure the base for 802.1x to perform access control on the specified interface. Use the **undo dot1x port-method** command to restore the default access control base.

By default, the value is **macbased**.

This command is used to set the base for 802.1x to perform access control, namely authenticate the users, on the specified interface. When **macbased** is used, the users accessing this interface must be authenticated independently, and as such will be able to access the network as long as they independently require. When **portbased** is used, only the first user on that port needs to be authenticated. Subsequent users accessing the network through this port are considered authenticated. However if the original user terminates his connection, the other users will need to be re-authenticated.

This command has an effect on the interface specified by the parameter *interface-list* when executed in System View. It has an effect on all the interfaces when no interface is specified. The parameter *interface-list* cannot be input when the command is executed in Ethernet Port View and it has an effect only on the current interface.

Related command: **display dot1x**.

Example

To authenticate the supplicant based on the port on Ethernet 1/0/3, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl-Z
[4500]dot1x port-method portbased interface ethernet 1/0/3
```

dot1x quiet-period

Command

dot1x quiet-period

undo dot1x quiet-period

View

System View

Parameter

None

Description

Use the **dot1x quiet-period** command to enable the quiet-period timer. Use the **undo dot1x quiet-period** command to disable this timer.

If an 802.1x user has not been authenticated, the Authenticator will keep quiet for a while (which is specified by quiet-period timer) before launching the authentication again. During the quiet period, the Authenticator does not do anything related to 802.1x authentication.

By default, the quiet-period timer is disabled.

Related command: **display dot1x**, **dot1x timer**.

Example

To enable quiet-period timer, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl-Z
[4500]dot1x quiet-period
```

dot1x retry

Syntax

dot1x retry ***max-retry-value***

undo dot1x retry

View

System View

Parameter

max-retry-value: Specifies the maximum times an Ethernet switch can retransmit the authentication request frame to the supplicant, ranging from 1 to 10.

By default, the value is 3, that is, the Switch can retransmit the authentication request frame to the supplicant 3 times.

Description

Use the **dot1x retry** command to configure the maximum times a Switch can retransmit the authentication request frame to the supplicant. Use the **undo dot1x retry** command to restore the default maximum retransmission time.

After the Switch has transmitted an authentication request frame to the user for the first time, if no user response is received during the specified time-range, the Switch will re-transmit authentication request to the user. This command is used to specify how many times the Switch can re-transmit the authentication request frame to the supplicant. When the time is 1, the Switch is configured to transmit the authentication request frame only once. 2 indicates that the Switch is configured to transmit authentication request frame once again when no response is received for the first time and so on. This command has an effect on all the ports after configuration.

Related commands: **display dot1x**.

Example

To configure the current device to transmit an authentication request frame to the user for no more than 9 times, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl-Z
[4500]dot1x retry 9
```

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

Ethernet Port View

Parameter

logoff: Cuts network connection to a user upon detecting the use of proxy.

trap: Sends a trap message upon detecting a user using proxy to access the Switch.

interface *interface-list*: Ethernet interface list including several Ethernet interfaces, expressed in the format ***interface-list* = { *interface-num* [to *interface-num*] } & < 1-10 >**. ***interface-num*** specifies a single Ethernet interface in the format ***interface-num* = { *interface-type interface-num* | *interface-name* }**, where ***interface-type*** specifies the interface type, ***interface-num*** specifies the interface number and ***interface-name*** specifies the interface name. For the respective meanings and value ranges, see the parameters in the Port Command chapter.

Description

Use the **dot1x supp-proxy-check** command to configure the control method for 802.1x proxy users on the specified interface. Use the **undo dot1x supp-proxy-check** command to cancel the control method set for 802.1x proxy users.

Note that when performing this function, the user logging on via proxy needs to run the 3Com 802.1x client program, (3Com 802.1x client program version V1.29 or above is needed).

This command is used to set a control method on the specified interface when executed in System View. The parameter *interface-list* cannot be input when the command is executed in Ethernet Port View and it takes effect only on the current interface. After globally enabling proxy user detection and control in System View, only if you enable this feature on a specific port can this configuration take effect on the port.

Related command: **display dot1x**.

Example

To configure the Switch to cut the network connection to a user upon detecting the use of proxy on Ethernet 1/0/1 ~ Ethernet 1/0/8, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]dot1x supp-proxy-check logoff
[4500]dot1x supp-proxy-check logoff interface Ethernet 1/0/1 to
Ethernet 1/0/8
```

To configure the Switch to send a trap message upon detecting the use of proxy to login to Ethernet 1/0/9, enter the following:

```
[4500]dot1x supp-proxy-check trap
[4500]dot1x supp-proxy-check trap interface ethernet 1/0/9
```

or

```
[4500]dot1x supp-proxy-check trap
[4500]interface Ethernet 1/0/9
[4500-ethernet1/0/9]dot1x supp-proxy-check trap
```

dot1x timer

Syntax

dot1x timer { handshake-period *handshake-period-value* | quiet-period *quiet-period-value* | tx-period *tx-period-value* | supp-timeout *supp-timeout-value* | server-timeout *server-timeout-value* }

undo dot1x timer { handshake-period | quiet-period | tx-period | supp-timeout | server-timeout }

View

System View

Parameter

handshake-period: This timer begins after the user has passed authentication. After setting the handshake-period, the system will send a handshake packet every handshake period seconds. Suppose the dot1x handshake-period time is configured as N, the system will consider the user as having logged off and will set the user state as logoff if the system does not receive a response from the user for N consecutive times.

handshake-period-value: Handshake period. The value ranges from 1 to 1024 in units of second and defaults to 15.

quiet-period: Specify the quiet timer. If an 802.1x user has not passed the authentication, the Authenticator will keep quiet for a while (which is specified by quiet-period timer) before launching the authentication again. During the quiet period, the Authenticator does not do anything related to 802.1x authentication.

quiet-period-value: Specify how long the quiet period is. The value ranges from 10 to 120 in units of second and defaults to 60.

server-timeout: Specify the timeout timer of an Authentication Server. If an Authentication Server has not responded before the specified period expires, the Authenticator will resend the authentication request.

server-timeout-value: Specify how long the duration of a timeout timer of an Authentication Server is. The value ranges from 100 to 300 seconds and defaults to 100 seconds.

supp-timeout: Specify the authentication timeout timer of a Supplicant. After the Authenticator sends Request/Challenge request packet which requests the MD5 encrypted text, the supp-timeout timer of the Authenticator begins to run. If the Supplicant does not respond back successfully within the time range set by this timer, the Authenticator will resend the above packet.

supp-timeout-value: Specify how long the duration of an authentication timeout timer of a Supplicant is. The value ranges from 10 to 120 seconds and defaults to 30 seconds.

tx-period: Specify the transmission timeout timer. After the Authenticator sends the Request/Identity request packet which requests the user name or user name and password together, timer of the Authenticator begins to run. If the Supplicant does not respond back with authentication reply packet successfully, then the Authenticator will resend the authentication request packet.

tx-period-value: Specify how long the duration of the transmission timeout timer is. The value ranges from 10 to 120 seconds and defaults to 30 seconds.

Description

Use the **dot1x timer** command to configure the 802.1x timers. Use the **undo dot1x timer** command to restore the default values.

802.1x has many timers that control the rational and orderly interacting of the Supplicant, the Authenticator and the Authentication Server. This command can set some of the timers (while other timers cannot be set) to adapt the interaction process. Changing the timers could be necessary in some special cases, but generally the user should keep the default values.

Related command: **display dot1x**.

Example

To set the Authentication Server timeout timer to 150s, enter the following:

```
<4500> system-view
System View: return to User View with Ctrl+Z.
[4500]dot1x timer server-timeout 150
```

reset dot1x statistics

Syntax

reset dot1x statistics [interface *interface-list*]

View

User View

Parameter

interface *interface-list*: Ethernet port list including several Ethernet ports. ***interface-list* = { *interface-num* [to *interface-num*] } & < 1-10 >**. ***interface-num*** specifies a single Ethernet port in the format ***port-num* = {**

interface-type interface-num | ***interface-name*** **}**, where ***interface-type*** specifies the port type, ***interface-num*** specifies the port number and ***interface-name*** specifies the port name. For the respective meanings and value ranges, read the Parameter of the Port Configuration section.

Description

Use the **reset dot1x statistics** command to reset the statistics of 802.1x.

This command can be used to re-perform statistics if the user wants to delete the former statistics of 802.1x.

When the original statistics are cleared, if no port type or port number is specified, the global 802.1x statistics of the Switch and 802.1x statistics on all the ports will be cleared. If the port type and port number are specified, the 802.1x statistics on the specified port will be cleared.

Related commands: **display dot1x**.

Example

Clear the 802.1x statistics on Ethernet 1/0/2.

```
<4500>reset dot1x statistics interface ethernet 1/0/2
```

Centralized MAC Address Authentication Configuration Commands

debugging mac-authentication event

Syntax

```
debugging mac-authentication event

undo debugging mac-authentication event
```

View

User View

Parameter

None

Description

Use the **debugging mac-authentication event** command to enable centralized MAC address authentication event debugging. Use the **undo debugging mac-authentication event** command to disable event debugging.

Example

To enable centralized MAC address authentication event debugging, enter the following:

```
<4500>debugging mac-authentication event
```

display mac-authentication

Syntax

display mac-authentication [interface *interface-list*]

View

Any view

Parameter

interface *interface-list*: Ethernet interface list including several Ethernet interfaces, expressed in the format ***interface-list* = { *interface-num* [to *interface-num*] } & < 1-10 >**. ***interface-num*** specifies a single Ethernet interface in the format ***interface-num* = { *interface-type interface-num* | *interface-name* }**, where ***interface-type*** specifies the interface type, ***interface-num*** specifies the interface number and ***interface-name*** specifies the interface name. For the respective meanings and value ranges, see the parameters in the Port Command chapter.

Description

Use the **display mac-authentication** command to display the global information on centralized MAC address authentication, including centralized MAC address authentication features, value of each current timer, number of online users, the MAC address in silent periods, and the authentication status of the MAC address on each interface.

Example

Display the global information of centralized MAC address authentication

```
<4500>display mac-authentication
mac address authentication is Enabled.
authentication mode is UsernameAsMacAddress
the Fixed username is mac
the Fixed password is NULL
         offline detect period is 300s
         quiet period is 1 minute
         server response timeout value  is 100s
         max allowed user number is 1024
         current user number amounts to  0
         current domain:
Silent Mac User info:
         MAC ADDR              From Port           Port Index
Ethernet1/0/1 is link-up
  MAC address authentication  is Disabled
  Authenticate success: 0, failed: 0
  Current online user number is 0
```

```
MAC ADDR          Authenticate state           AuthIndex
```

Table 29 Description of MAC address authentication configuration information

Field	Description
`mac address authentication is Enabled`	The centralized MAC address authentication feature is enabled on the switch
`authentication mode`	The centralized MAC address authentication mode. By default, it is MAC address mode.
`the Fixed username`	The username for fixed mode. By default, the username is mac.
`the Fixed password`	The password for fixed mode. By default it is not configured.
`offline detect period`	Offline-detect timer, set the time interval for the Switch to detect whether the user is offline. By default, it is 300 seconds.
`quiet period`	Quiet timer. A period of quiet time that the Switch needed after failing to authenticate the user. By default, it is 1 minute.
`server response timeout value`	Server timeout timer, set the timeout period to the connection between the Switch to the RADIUS server. By default, it is 100 seconds.
`max allowed user number`	The maximum number of users allowed by the Switch.
`current user number amounts`	Current user number.
`current domain`	Current domain, by default, it is not configured.
`Silent Mac User info`	The silent user information. If a user does not pass the MAC address authentication, the Switch sets this user to be silent, in this period of time, the Switch does not authenticate this user.
`Ethernet1/0/1 is link-up`	Interface Ethernet1/0/1 link is in the up state.
`MAC address authentication is Enabled`	MAC address authentication is enabled on interface Ethernet1/0/1
`Authenticate success: 0, failed: 0`	The statistics of the MAC address authentication on the interface, including the number of users passing the authentication and the number of users failing the authentication.
Authenticate state	There are four states of the online users: ■ Connecting: the user is connecting ■ Success: the user has passed the authentication ■ Failure: the user has failed the authentication ■ Logoff: the user is offline.

mac-authentication

Syntax

`mac-authentication [ interface` ***`interface-list`*** **`]`**

`undo mac-authentication [ interface` ***`interface-list`*** **`]`**

View

Ethernet Port View

Parameter

interface *interface-list:* Ethernet interface list including several Ethernet interfaces, expressed in the format ***interface-list* = { *interface-num* [to *interface-num*] } & < 1-10 >**. ***interface-num*** specifies a single Ethernet interface in the format ***interface-num* = { *interface-type interface-num* | *interface-name* }**, where ***interface-type*** specifies the interface type, ***interface-num*** specifies the interface number and ***interface-name*** specifies the interface name. For the respective meanings and value ranges, see the parameters in the Port Command chapter.

Description

Use the **mac-authentication** command to enable the centralized MAC address authentication feature on a specified port or globally. Use the **undo mac-authentication** command to disable the feature on a specified port or globally.

By default, the centralized MAC address authentication feature is disabled on each port and globally.

In System View, if the ***interface-list*** parameter is not specified, the centralized MAC address authentication feature is enabled globally; if the ***interface-list*** parameter is specified, the feature is enabled on the specified interfaces. In the Ethernet Port View, the ***interface-list*** parameter cannot be specified, and you can use the command only to enable the feature on the current interface.

Before or after the enabling of the centralized MAC address authentication, you can configure related parameters both globally or on the port through their respective commands. If the parameters are not configured before enabling this feature, then the parameters will be in their default state when it is enabled.

You must first enable the centralized MAC address authentication globally and then on the port to make the related configurations on the port effective.

Example

To enable the centralized MAC address authentication feature on port Ethernet 1/0/1, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]mac-authentication interface Ethernet 1/0/1
```

To enable the centralized MAC address authentication feature globally, enter the following:

```
[4500]mac-authentication
```

mac-authentication authmode

Syntax

mac-authentication authmode { *usernameasmacaddress* | *usernamefixed* }

undo mac-authentication authmode

View

System View

Parameter

***usernamemacaddress*:** Specify the MAC address mode for authentication.

usernamefixed: Specify the fixed mode for authentication.

Description

Use the **mac-authentication authmode** command to set the MAC address authentication mode. Use the **undo mac-authentication authmode** command to remove the configuration.

- If you set the authentication mode to **usernameasmacaddress**, the MAC address mode is used for authentication (both the username and password are the MAC address of the user).
- If you set the authentication mode to **usernamefixed**, the fixed mode is used for authentication (both the username and password are pre-defined).

By default, the MAC address authentication mode is **usernameasmacaddress**.

Example

To set the MAC address authentication mode to usernamefixed, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]mac-authentication authmode usernamefixed
```

mac-authentication authpassword

Syntax

mac-authentication authpassword *password*

undo mac-authentication authpassword

View

System View

Parameter

password: Password for authentication, a string ranging from 1 to 16 characters in length.

Description

Use the **mac-authentication authpassword** command to set the password to use when the centralized MAC authentication mode is set to usernamefixed.

Use the undo **mac-authentication authpassword** command to remove the configured password.

By default, the password is configured when the centralized MAC authentication mode is set to **usernamefixed**.

Example

To set the password for the fixed mode to mac, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]mac-authentication authpassword mac
```

mac-authentication authusername

Syntax

mac-authentication authusername *text*

undo mac-authentication authusername

View

System View

Parameter

text: User name for authentication, a string ranging from 1 to 55 characters in length.

Description

Use the **mac-authentication authusername** command to set the user name to use when the MAC authentication mode is set to usernamefixed.

Use the **undo mac-authentication authusername** command to restore the default user name.

By default, the user name for the fixed MAC address authentication mode is mac.

Example

To set the user name for the fixed mode to vip user, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]mac-authentication authusername vipuser
```

To restore the default user name for the fixed mode, enter the following:

```
[4500]undo mac-authentication authusername
```

mac-authentication domain

Syntax

mac-authentication domain *isp-name*

undo mac-authentication domain

View

System View

Parameter

isp-name: ISP domain name, character string with no more than 24 characters, excluding characters like "/", ":", "*", "?", "<", and ">".

Description

Use the **mac-authentication domain** command to configure the ISP domain used by the centralized MAC address authentication user. Use the **undo mac-authentication domain** command to return to the default ISP domain.

By default, the domain used by centralized MAC address authentication user is null, that is, not configured.

Example

To configure the domain used by the MAC address to Cams, enter the following:

```
<4500> system-view
System View: return to User View with Ctrl+Z.
[4500]mac-authentication domain Cams
```

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

Parameter

offline-detect: Offline-detect timer, set the time interval for the Switch to detect whether the user is offline.

offline-detect-value: Period set by the offline-detect timer, ranging from 1 to 65535, in seconds. The default value is 300 seconds.

quiet: Quiet timer. If the user fails authentication, the Switch needs a period of quiet time (set by the quiet timer) before it re-authenticates. The Switch does not authenticate during the quiet time.

quiet-value: Period set by the quiet timer, ranging from 1 to 65535, in seconds. The default value is 60.

server-timeout: Server timeout timer. During the authentication to the user, if the connection between the Switch and the RADIUS server times out, the Switch denies the user's access to the network on corresponding ports.

server-timeout-value: Period set by the server timeout timer, ranging form 1 to 65535, in seconds. The default value is 100 seconds.

Description

Use the **mac-authentication timer** command to configure timer parameters of the centralized MAC address authentication. Use the **undo mac-authentication timer** command to restore the value to the defaults.

For the related command, see **display mac-authentication**.

Example

To set the timeout timer of the server to 150 seconds, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]mac-authentication timer server-timeout 150
```

AAA and RADIUS Configuration Commands

This section describes how to use the AAA and RADIUS configuration commands on your Switch 4500.

access-limit

Syntax

access-limit { disable | **enable *max-user-number* }**

View

ISP Domain View

Parameter

disable: No limit to the supplicant number in the current ISP domain.

enable *max-user-number:* Specifies the maximum supplicant number in the current ISP domain, ranging from 1 to 1048

Description

Use the **access-limit** command to configure a limit to the amount of supplicants in the current ISP domain.

By default, there is no limit to the amount of supplicants in the current ISP domain.

This command limits the amount of supplicants contained in the current ISP domain. The supplicants may contend with each other for the network resources. So setting a suitable limit to the amount will guarantee the reliable performance for the existing supplicants.

Example

Sets a limit of 500 supplicants for the ISP domain, marlboro.net.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]domain marlboro.net
New domain added.
[4500-isp-marlboro.net]access-limit enable 500
```

attribute

Syntax

attribute { ip *ip-address* | mac *mac-address* | idle-cut *second* | access-limit *max-user-number* | vlan *vlanid* | location { nas-ip *ip-address* port *portnum* | port *portnum* }

undo attribute {ip | mac | idle-cut | access-limit | vlan | location }

View

Local User View

Parameter

ip: Specifies the IP address of a user.

mac *mac-address:* Specifies the MAC address of a user. Where, ***mac-address*** takes on the hexadecimal format of ***HHHH-HHHH-HHHH-HHHH***.

idle-cut *second:* Allows/disallows the local users to enable the idle-cut function. (The specific data for this function depends on the configuration of the ISP domain where the users are located.) The argument ***minute*** defines the idle-cut time, which is in the range of 60 to 7200 seconds.

access-limit *max-user-number:* Specifies the maximum number of users who access the device using the current user name. The argument ***max-user-number*** is in the range of 1 to 1024.

vlan *vlanid:* Sets the VLAN attribute of user, in other words, the VLAN to which a user belongs. The argument ***vlanid*** is an integer in the range of 1 to 4094.

location: Sets the port binding attribute of user.

nas-ip *ip-address:* The IP address of the access server in the event of binding a remote port with a user. The argument ***ip-address*** is an IP address in dotted decimal format and defaults to 127.0.0.1.

port *portnum:* Sets the port to which a user is bound. The argument ***portnum*** is represented by "SlotNumber SubSlotNumber PortNumber". If any of these three items is absent, the value 0 will be used to replace it.

Description

Use the **attribute** command to configure some attributes for specified local user. Use the **undo attribute** command to cancel the attributes that have been defined for this local user.

It should be noted that the argument nas-ip must be defined for a user bound with a remote port, which is unnecessary, however, in the event of a user bound with a local port.

Related command: **display local-user**.

Example

To configure the IP address 10.110.50.1 to the user JohnQ, enter the following:

```
<4500> system-view
System View: return to User View with Ctrl+Z.
[4500]local-user JohnQ
New local user added.
[4500-luser-JohnQ]ip 10.110.50.1
```

cut connection

Syntax

cut connection { all | **access-type { dot1x** | **mac-authentication } |** **domain *domain-name*** | **interface *interface-type interface-number*** | **ip *ip-address*** | **mac *mac-address*** | **radius-scheme *radius-scheme-name*** | **vlan *vlanid*** | **ucibindex *ucib-index*** | **user-name *user-name* }**

View

System View

Parameter

all: Configures to disconnect all connection.

access-type { dot1x | mac authentication }: Configures to cut a category of connections according to logon type. **dot1x** means the 802.1x users. **mac authentication** means the centralized MAC address authentication users.

domain *domain-name:* Configures to cut the connection according to ISP domain. ***domain-name*** specifies the ISP domain name with a character string not exceeding 24 characters. The specified ISP domain shall have been created.

mac *mac-address:* Configures to cut the connection of the supplicant whose MAC address is ***mac-address***. The argument ***mac-address*** is in the hexadecimal format (H-H-H).

radius-scheme *radius-scheme-name:* Configures to cut the connection according to RADIUS server name. ***radius-scheme-name*** specifies the RADIUS server name with a character string not exceeding 32 characters.

interface *interface-type interface-number:* Configures to cut the connection according to the port.

ip *ip-address:* Configures to cut the connection according to IP address. The argument ***ip-address*** is in the hexadecimal format (ip-address).

vlan *vlanid:* Configures to cut the connection according to VLAN ID. Here, ***vlanid*** ranges from 1 to 4094.

ucibindex *ucib-index:* Configures to cut the connection according to ***ucib-index***. Here, ***ucib-index*** ranges from 0 to 1047.

user-name *user-name:* Configures to cut the connection according to user name. ***user-name*** is the argument specifying the username. It is a character string not exceeding 80 characters, excluding "/", ":", "*", "?", "<" and ">". The @ character can only be used once in one username. The pure username (the part before @, namely the user ID) cannot exceed 55 characters.

Description

Use the **cut connection** command to disconnect a user or a category of users by force.

Related command: **display connection**.

Example

To cut all the connections in the ISP domain, marlboro.net, enter the following:

```
<4500> system-view
System View: return to User View with Ctrl+Z.
[4500]cut connection domain marlboro.net
```

display connection

Syntax

display connection [access-type { dot1x | mac-authentication } | domain *domain-name* | interface *interface-type interface-number* | ip

ip-address | **mac** ***mac-address*** | **radius-scheme** ***radius-scheme-name*** | **vlan** ***vlanid*** | **ucibindex** ***ucib-index*** | **user-name** ***user-name*** **]**

View

All views

Parameter

access-type { dot1x | **mac-authentication }:** Configures to display the supplicants according to their logon type. **dot1x** means the 802.1x users. **mac-authentication** means the centralized mac address authentication users.

domain ***domain-name:*** Configures to display all the users in an ISP domain. ***domain-name*** specifies the ISP domain name with a character string not exceeding 24 characters. The specified ISP domain shall have been created.

mac ***mac-address:*** Configures to display the supplicant whose MAC address is ***mac-address***. The argument ***mac-address*** is in the hexadecimal format (*H-H-H*).

radius-scheme ***radius-scheme-name:*** Configures to display the supplicant according to RADIUS server name. ***radius-scheme-name*** specifies the RADIUS server name with a character string not exceeding 32 characters.

interface ***interface-type interface-number:*** Configures to display the supplicant according the port.

ip ***ip-address:*** Configures to display the user specified with IP address. The argument ***ipt-address*** is in the hexadecimal format (ip-address).

vlan ***vlanid:*** Configures to display the user specified with VLAN ID. Here, ***vlanid*** ranges from 1 to 4094.

ucibindex ***ucib-index:*** Configures to display the user specified with ***ucib-index***. Here, ***ucib-index*** ranges from 0 to 1047.

user-name ***user-name:*** Configures to display a user specifies with ***user-name***. ***user-name*** is the argument specifying the username. It is a character string not exceeding 32 characters.

Description

Use the **display connection** command to view the relevant information of all the supplicants or the specified one(s).

The output can help you with the user connection diagnosis and troubleshooting.

If no parameter is specified, this command displays the related information about all connected users

Related command: **cut connection**.

Example

To display the relevant information of all the users, enter the following:

```
<4500>display connection
Total 0 connections matched ,0 listed.
```

display domain

Syntax

display domain [*isp-name*]

View

All views

Parameter

isp-name: Specifies the ISP domain name, with a character string not exceeding 24 characters. The specified ISP domain shall have been created.

Description

Use the **display domain** command to view the configuration of a specified ISP domain or display the summary information of all ISP domains.

This command is used to output the configuration of a specified ISP domain or display the summary information of all ISP domains. If an ISP domain is specified, the configuration information (content and format) will be displayed exactly the same as the displayed information of the **display domain** command. The output information can help with ISP domain diagnosis and troubleshooting. Note that the accounting scheme to be displayed should have been created.

Related commands: **access-limit**, **domain**, **radius scheme**, **state**, **display domain**.

Example

To display the summary information of all ISP domains of the system, enter the following:

```
<4500>display domain
0  Domain = system
   State = Active
   Access-limit = Disable
   Scheme = LOCAL
   Domain User Template:
   Idle-cut = Disable
   Self-service = Disable
   Messenger Time = Disable
Default Domain Name: system
Total 1 domain (s). 1 listed.
```

display local-user

Syntax

display local-user [domain *isp-name* | idle-cut { enable | disable } | service-type { telnet | ftp | ssh | terminal | lan-access } | state { active | block } | user-name *user-name* | vlan *vlanid*]

View

All views

Parameter

domain *isp-name:* Configures to display all the local users in the specified ISP domain. ***isp-name*** specifies the ISP domain name with a character string not exceeding 24 characters. The specified ISP domain shall have been created.

idle-cut: Configures to display the local users according to the state of idle-cut function. **disable** means that the user disables the idle-cut function and **enable** means the user enables the function. This parameter only takes effect on the users configured as lan-access type. For other types of users, the **display local-user idle-cut enable** and **display local-user idle-cut disable** commands do not display any information.

service-type: Configures to display local user of a specified type. **telnet** means that the specified user type is telnet. **ftp** means that the specified user type is ftp. **ssh** means the specified user type is ssh. **terminal** means that the specified user type is terminal which refers to users who use the terminal service (login from the console port). **lan-access** means that the specified user type is lan-access which mainly refers to Ethernet accessing users, 802.1x supplicants for example.

state { active | **block }:** Configures to display the local users in the specified state. **active** means that the system allows the user requesting network service and **block** means the system does not allow the user requesting network service.

user-name ***user-name:*** Configures to display a user specified with ***user-name***. ***user-name*** is the argument specifying the username. It is a character string not exceeding 80 characters.

vlan ***vlanid*****:** Configures to display the users bound to the specified VLAN. ***vlanid*** is the integer, ranging from 1 to 4094.

Description

Use the **display local-user** command to view the relevant information of all the local users or the specified one(s).

This command displays the relevant information about a specified or all the local users. The output can help you with the fault diagnosis and troubleshooting related to local user.

Related command: **local-user**.

Example

To display the relevant information of all the local users, enter the following:

```
<4500>display local-user
The contents of local user xxx:
 State:          Active            ServiceType Mask:
 Idle Cut:       Disable
 AccessLimit:    Disable           Current AccessNum: 0
 Bind location:  Disable
 Vlan ID:        Disable
Total 1 local user(s) Matched,1 listed.
```

Table 30 Output description of the **display local-user** command

Field	Description
State	The state of the user
Idle-Cut	The state of the idle-cut Switch
Access-Limit	The limit of the number of access users
Bind location	Indicates whether a port is bound with or not
VLAN ID	The ID of the VLAN to which the user is bound
IP address	The bound ip address of the user
MAC address	The bound MAC address of the user
FTP Directory	The directory authorized to FTP users

domain

Syntax

domain { *isp-name* | default { disable | enable *isp-name* }}
undo domain *isp-name*

View

System View

Parameter

***isp-name*:** Specifies an ISP domain name. The name is expressed with a character string not exceeding 24 characters, excluding "/", ": ", "*", "? ", "<", and ">".

default enable *isp-name*: Enables the default ISP domain specified by ***isp-name***.

default disable: Restores the default ISP domain to **system**.

Description

Use the **domain** command to configure an ISP domain or enter the view of an existing ISP domain. Use the **undo domain** command to cancel a specified ISP domain.

By default, a domain named ***system*** has been created in the system. The attributes of ***system*** are all default values.

ISP domain is a group of users belonging to the same ISP. Generally, for a username in the userid@isp-name format, taking gw20010608@3Com163.net as an example, the isp-name (that is, 3Com163.net) following the @ is the ISP domain name. When 3Com 4500 Series Ethernet Switches control user access, as for an ISP user whose username is in userid@isp-name format, the system will take userid part as username for identification and take isp-name part as domain name.

The purpose of introducing ISP domain settings is to support the application environment with several ISP domains. In this case, an access device may have supplicants from different ISP domains. Because the attributes of ISP users, such as username and password structures, service types, may be different, it is necessary to separate them by setting ISP domains. In ISP Domain View, you can configure a complete set of exclusive ISP domain attributes for each ISP domain, which includes AAA schemes (RADIUS scheme applied and so forth.)

For a Switch, each supplicant belongs to an ISP domain. The system supports up to 16 ISP domains. If a user has not reported its ISP domain name, the system will put it into the default domain.

When this command is used, if the specified ISP domain does not exist, the system will create a new ISP domain. All the ISP domains are in the **active** state when they are created.

Related commands: **access-limit**, **radius scheme**, **state**, **display domain**.

Example

To create a new ISP domain, marlboro.net, and enters its view, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]domain marlboro.net
New Domain added.
[4500-isp-marlboro.net]
```

idle-cut

Syntax

idle-cut { disable | **enable** ***minute flow*** **}**

View

ISP Domain View

Parameter

disable: means disabling the user to use idle-cut function .

enable: means enabling the user to use the function.

minute: Specifies the maximum idle time, ranging from 1 to 120 and measured in minutes.

flow: The minimum data traffic, ranging from 1 to 10,240,000 and measured in bytes.

Description

Use the **idle-cut** command to configure the user template in the current ISP domain.

By default, after an ISP domain is created, this attribute in user template is **disable**, that is, the user idle-cut is disabled.

The user template is a set of default user attributes. If a user requesting for the network service does not have some required attributes, the corresponding attributes in the template will be endeavored to him as default ones. The user template of the Switch you are using may only provide user idle-cut settings. After a user is authenticated, if the idle-cut is configured to enable or disable by neither the user nor the RADIUS server, the user will adopt the idle-cut state in the template.

Because a user template only works in one ISP domain, it is necessary to configure user template attributes for users from different ISP domain respectively.

Related command: **domain**

Example

To enable the user in the current ISP domain, 3Com163.net, to use the idle-cut attribute specified in the user template (that is, enabling the user to use the idle-cut function). The maximum idle time is 50 minutes and the minimum data traffic is 500 bytes.

```
<4500> system-view
System View: return to User View with Ctrl+Z.
[4500]domain marlboro.net
[4500-isp-marlboro.net]idle-cut enable 50 500
```

level

Syntax

level ***level***

undo level

View

Local User View

Parameter

***level*:** Specifies user priority level, an integer ranging from 0 to 3.

Description

Use the **level** command to configure user priority level. Use the **undo level** command to restore the default user priority level.

By default, the user priority level is 0.

Related command: **local-user**

If the configured authentication mode is none authentication or password authentication, the command level that a user can access after login depends on the priority of user interface. In the case of authentication requiring both username and password, however, the accessible command level depends on user priority level.

Example

To set the priority level of the user 3Com to 3, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]local-user 3Com1
[4500-luser-3Com1]level 3
```

local-user

Syntax

local-user ***user-name***

undo local-user { *user-name* | all [service-type { telnet | ftp | lan-access | ssh | terminal }] }

View

System View

Parameter

user-name: Specifies a local username with a character string not exceeding 80 characters, excluding "/", ":", "*", "?", "<" and ">". The @ character can only be used once in one username. The pure username (the part before @, namely the user ID) cannot exceed 55 characters. The ***user-name*** parameter is not case sensitive.

service-type: Specifies the service type.

telnet: The specified user type is telnet.

ftp: The specified user type is ftp.

lan-access: The specified user type is lan-access which mainly refers to Ethernet accessing users, 802.1x supplicants for example.

ssh: The specified user type is ssh.

terminal: The specified user type is terminal which refers to users who use the terminal service (login from the console port).

all: All the users.

Description

Use the **local-user** command to configure a local user and enter the local user view. Use the **undo local-user** command to cancel a specified local user.

By default, no local user.

Related commands: **display local-user**, **server-type**.

Example

To add a local user named 3Com1, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]local-user 3Com1
[4500-luser-3Com1]
```

local-user password-display-mode

Syntax

local-user password-display-mode { cipher-force | auto }

undo local-user password-display-mode

View

System View

Parameter

cipher-force: Forced cipher mode specifies that the passwords of all the accessed users must be displayed in cipher text.

auto: The auto mode specifies that a user is allowed to use the password command to set a password display mode.

Description

Use the **local-user password-display-mode** command, you can configure the password display mode of all the accessing user. Use the **undo local-user password-display-mode** command to cancel password display mode that has been set for all the accessing users.

The password display mode of all the accessing users defaults to **auto**.

Related commands: **display local-user**, **password**

Example

To force all accessing users to display passwords in cipher text, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]local-user password-display-mode cipher-force
```

messenger

Syntax

messenger time { enable ***limit interval*** | **disable }**
undo messenger time

View

ISP Domain View

Parameter

limit: Remaining-online-time threshold in minutes, in the range of 1 to 60. When the remaining online time of a user is equal to this threshold, the Switch begins to send alert messages to the client.

interval: Sending interval of alert messages in minutes, in the range of 5 to 60 (must be a multiple of 5).

Description

Use the **messenger time enable** command to enable messenger alert and configure the related parameters.

Use the **messenger time disable** command to disable messenger alert.

Use the **undo messenger time** command to restore messenger alert to default settings.

By default, the messenger alert is disabled on the Switch.

This function allows the clients to inform the online users about their remaining online time through message alert dialog box.

The implementation of this function is as follows:

- On the Switch, use the **messenger time enable** command to enable this function and to configure the remaining-online-time threshold (the ***limit*** argument) and the alert message interval.
- If the threshold is reached, the Switch sends messages containing the user's remaining online time to the client at the interval you configured.

- The client keeps the user informed of the remaining online time through a message alert dialog box.

Example

To configure to start the sending of alert messages when the user's remaining online time is 30 minutes and send the messages at an interval of five minutes, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]domain system
[4500-isp-system]messenger time enable 30 5
```

password

Syntax

password { simple | **cipher } *password***

undo password

View

Local User View

Parameter

cipher: Configure to display passwords in encrypted text.

simple: Configure to display passwords in plain text.

password: Defines a password. For **simple** mode, the password must be in plain text. For **cipher** mode, the password can be either in encrypted text or in plain text. The result is determined by the input. A plain text password is a character string of no more than 16 characters.

Description

Use the **password** command to configure a password display mode for local users. Use the **undo password** command to cancel the specified password display mode.

Related command: **display local-user**.

Example

To set the user 3Com1 to display the password in simple text, given the password is 20030422, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]local-user 3Com1
[4500-luser-3Com1]password simple 20030422
```

radius-scheme

Syntax

radius-scheme *radius-scheme-name*

View

ISP Domain View

Parameter

radius-scheme-name: Specifies a RADIUS scheme, with a character string not exceeding 32 characters.

Description

Use the **radius-scheme** command to configure the RADIUS scheme used by the current ISP domain.

This command is used to specify the RADIUS scheme for the current ISP domain. The specified RADIUS scheme shall have been created.

Related commands: **radius scheme**, **display radius**.

Example

The following example designates the current ISP domain, marlboro.net, to use the RADIUS server, Radserver.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]domain marlboro.net
[4500-isp-marlboro.net]radius-scheme Radserver
```

scheme

Syntax

scheme { radius-scheme *radius-scheme-name* [local] | local | none }

undo scheme { radius-scheme | none }

View

ISP Domain View

Parameter

radius-scheme-name: RADIUS scheme, a character string not exceeding 32 characters.

local: Local authentication.

none: No authentication.

Description

Use the **scheme** command to configure the AAA scheme to be referenced by the current ISP domain. Use the **undo scheme** command to restore the default AAA scheme.

The default AAA scheme in the system is local.

The system adopts three types of AAA schemes to perform authentication and/or accounting: local authentication, no authentication and RADIUS scheme.

- When using **radius-scheme *radius-scheme-name* local** in the configuration command, the **local** refers to the alternative authentication scheme if the RADIUS server does not respond normally. Therefore, when the RADIUS server operates normally, the local scheme is not used otherwise, the local scheme is used.

- If the **local** or **none** scheme applies, no RADIUS scheme can be adopted.
- If you want to specify the ISP domain to adopt RADIUS scheme, then the RADIUS scheme must have already been configured.

You can use either **scheme** or **radius-scheme** command to specify the RADIUS scheme for an ISP domain. If both of these two commands are used, the latest configuration will take effect.

Related command: **radius scheme**, **display radius**

Example

To specify the current ISP domain, 3Com163.net, to use the RADIUS scheme 3Com, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]domain marlboro.net
[4500-isp-marlboro.net]scheme radius-scheme 3Com
```

self-service-url

Syntax

self-service-url enable ***url-string***
self-service-url disable

View

ISP Domain View

Parameter

url-string: The URL address of the page used to change the user password on the self-service server, a string with 1 to 64 characters. This string cannot contain "?" character. If "?" is contained in the URL address, you must replace it with "|" when inputting the URL address in the command line.

Description

Use the **self-service-url enable** command to configure self-service server URL.

Use the **self-service-url disable** command to remove the configuration.

By default, self-service server URL is not configured on the Switch.

This command must be incorporated with a RADIUS server (such as a CAMS server) that supports self-service. Self-service means that users can manage their accounts and card numbers by themselves. And a server with the self-service software is called a self-service server.

Once this function is enabled on the Switch, users can locate the self-service server and perform self-management through the following operations:

- Select "Change user password" on the 802.1x client.
- After the client opens the default explorer (IE or NetScape), locate the specified URL page used to change the user password on the self-service server.
- Change user password on this page.

The "Change user password" option is available only after the user passed the authentication; otherwise, this option is in grey and unavailable.

Example

In the ISP domain "marlboro.net", configure the URL address of the page used to change the user password on the self-service server to http://10.153.89.94/selfservice/modPasswd1x.jsp|userName.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]domain marlboro.net
[4500-isp-marlboro.net] self-service-url enable
http://10.153.89.94/selfservice/modPasswd1x.jsp|userName
```

service-type

Syntax

```
service-type { ftp [ ftp-directory directory ] | lan-access | ssh |
telnet [ level level ] }

undo service-type { ftp [ ftp-directory ] | lan-access | { ssh |
telnet * }
```

View

Local User View

Parameter

telnet: Specifies user type as Telnet.

level *level*: Specifies the level of Telnet users. The argument ***level*** is an integer in the range of 0 to 3 and defaults to 0.

ftp: Specifies user type as ftp.

ftp-directory *directory*: Specifies the directory of ftp users, ***directory*** is a character string of up to 64 characters.

lan-access: Specifies user type to lan-access, which mainly refers to Ethernet accessing users, 802.1x supplicants for example.

ssh: The specified user type is ssh.

Description

Use the **service-type** command to configure a service type for a particular user. Use the **undo service-type** command to cancel the specified service type for the user.

When you configure the service type ssh, Telnet or Terminal, note the following:

- When you configure a new service type for a user, the system adds the new service type to the existing one.
- You can set a user level when you configure a service type. If you set multiple service types and specify the user levels, only the last configured user level is valid. Service types do not have individual user levels.

You can use either **level** *or* **service-type** *commands to specify the level for a local user. If both of these commands are used, the latest configuration takes effect.*

Example

To set to provide the lan-access service for the user JohnQ, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]local-user JohnQ
[4500-luser-JohnQ]service-type lan-access
```

state

Syntax

state { active | **block }**

View

ISP Domain View

Local User View

Parameter

active: Configures the current ISP domain (ISP Domain View)/current user (Local User View) as being in active state, that is, the system allows the users in the domain (ISP Domain View) or the current user (Local User View) to request network service.

block: Configures the current ISP domain (ISP Domain View)/current user (Local User View) as being in block state, that is, the system does not allow the users in the domain (ISP Domain View) or the current user (Local User View) to request network service.

Description

Use the **state** command to configure the state of the current ISP domain/current user.

By default, after an ISP domain is created, it is in the **active** state (in ISP Domain View).

A local user will be **active** (in Local User View) upon its creation.

In ISP Domain View, every ISP can either be in active or block state. If an ISP domain is configured to be active, the users in it can request for network service, while in block state, its users cannot request for any network service, which will not affect the users currently online.

Related command: **domain**.

Example

To set the current ISP domain marlboro.net to be in the block state. The supplicants in this domain cannot request for the network service, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
```

```
[4500]domain marlboro.net
[4500-isp-marlboro.net]state block
[4500-isp-marlboro.net]quit
```

To set the user 3Com1 to be in the block state, enter the following:

```
[4500-user-3Com1]state block
```

RADIUS Protocol Configuration Commands

This section describes how to use the RADIUS Protocol configuration commands on your Switch.

accounting optional

Syntax

accounting optional
undo accounting optional

View

ISP Domain View

Parameter

None

Description

Use the **accounting optional** command to enable the selection of the RADIUS accounting option. Use the **undo accounting optional** command to disable the selection of RADIUS accounting option.

By default, selection of the RADIUS accounting option is disabled.

If no RADIUS server is available or if RADIUS accounting server fails when the accounting optional is configured, the user can still use the network resource, otherwise, the user will be disconnected.

The user configured with **accounting optional** command in RADIUS scheme will no longer send real-time accounting update packet or stop accounting packet.

The **accounting optional** command in RADIUS Scheme View is only effective on the accounting that uses this RADIUS scheme.

Example

Enable the selection of RADIUS accounting of the RADIUS scheme named as CAMS.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]radius scheme cams
New Radius scheme
[4500-radius-cams]accounting optional
```

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

Parameter

data: Set data unit.

byte: Set 'byte' as the unit of data flow.

giga-byte: Set 'giga-byte' as the unit of data flow.

kilo-byte: Set 'kilo-byte' as the unit of data flow.

mega-byte: Set 'mega-byte' as the unit of data flow.

packet: Set data packet unit.

giga-packet: Set 'giga-packet' as the unit of packet flow.

kilo-packet: Set 'kilo-packet' as the unit of packet flow.

mega-packet: Set 'mega-packet' as the unit of packet flow.

one-packet: Set 'one-packet' as the unit of packet flow.

Description

- Use the **data-flow-format** command to configure the unit of data flow that is sent to the RADIUS Server.
- Use the **undo data-flow format** command to restore the unit to the default setting.

By default, the data unit is byte and the data packet unit is one-packet.

Related command: **display radius**.

Example

To set the unit of data flow that is sent to kilo-byte and the data packet to kilo-packet, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]radius scheme 3Com
New Radius scheme
[4500-radius-3Com]data-flow-format data kilo-byte packet kilo-packet
```

display local-server statistics

Syntax

display local-server statistics

View

All views

Parameter

None

Description

Use the **display local-server statistics** command to view the statistics of local RADIUS authentication server.

Related command: **local-server**.

Example

To display the statistics of local RADIUS authentication server, enter the following

```
<4500>display local-server statistics
The localserver packet statistics:
Receive:                  0          Send:                     0
Discard:                  0          Receive Packet Error:     0
Auth Receive:             0          Auth Send:                0
Acct Receive:             0          Acct Send:                0
```

display radius

Syntax

display radius [***radius-scheme-name*** **]**

View

All views

Parameter

radius-scheme-name: Specifies the RADIUS scheme name with a character string not exceeding 32 characters. Display all RADIUS schemes when the parameter is not set.

Description

Use the **display radius** command to view the configuration information of all RADIUS schemes or a specified one.

By default, this command outputs the configuration information about the specified or all the RADIUS schemes. The output can help with RADIUS diagnosis and troubleshooting.

Related command: **radius scheme**.

Example

To display the configuration information of all the RADIUS schemes, enter the following.

```
<4500>display radius
------------------------------------------------------------------
SchemeName  =system                           Index=0    Type=3Com
Primary Auth IP  =127.0.0.1        Port=1645   State=active
Primary Acct IP  =127.0.0.1        Port=1646   State=active
Second  Auth IP  =0.0.0.0          Port=1812   State=active
Second  Acct IP  =0.0.0.0          Port=1813   State=active
Auth Server Encryption Key= 3Com
Acct Server Encryption Key= 3Com
Accounting method = required
```

```
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
------------------------------------------------------------------
Total 1 RADIUS scheme(s). 1 listed
```

display radius statistics

Syntax

display radius statistics

View

All views

Parameter

None

Description

Use the **display radius statistics** command to view the statistics information of RADIUS packet.

This command outputs the statistics information about the RADIUS packets. The displayed packet information can help with RADIUS diagnosis and troubleshooting.

Related command: **radius scheme**.

Example

To display the statistics information of RADIUS packets, enter the following:

```
<4500>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
Receive and Send packets statistic:
Send PKT total  :0        Receive 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
Code=22,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
Leaving request                 ,Num=0       ,Err=0       ,Succ=0
```

```
PKT auth timeout                ,Num=0       ,Err=0       ,Succ=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

All views

Parameter

radius-scheme *radius-scheme-name*: Configures to display the saved stopping accounting requests according to RADIUS server name. ***radius-scheme-name*** specifies the RADIUS server name with a character string not exceeding 32 characters.

session-id *session-id*: Configures to display the saved stopping accounting requests according to the session ID. ***session-id*** specifies the session ID with a character string not exceeding 50 characters.

time-range *start-time stop-time*: Configures to display the saved stopping accounting requests according to the saving time. ***Start-time*** specifies the start time of the saving time range and ***stop-time*** specifies the stop time of the saving time range. The time is expressed in the format hh:mm:ss-yyyy/mm/dd. When this parameter is specified, all the stopping accounting requests saved in the time range since ***start-time*** to ***stop-time*** will be displayed.

user-name *user-name*: Configures to display the saved stopping accounting requests according to the username. ***User-name*** specifies the username, a character string not exceeding 32 characters.

Description

Use the **display stop-accounting-buffer** command to view the stopping accounting requests, which have not been responded and saved in the buffer.

After transmitting the stopping accounting requests, if there is no response from the RADIUS server, the Switch will save the packet in the buffer and retransmit it for several times, which is set through the **retry realtime-accounting**.

This command is used to display the stopping accounting requests saved in the Switch buffer. You can select to display the packets sent to a certain RADIUS server, or display the packets according to user session ID or username. You may also display the request packets saved during a specified time range. The displayed packet information can help with diagnosis and troubleshooting.

Related commands: **reset stop-accounting-buffer**, **stop-accounting-buffer enable**, **retry stop-accounting**.

Example

To display the stopping accounting requests saved in the system buffer since 0:0:0 to 23:59:59 on August 31, 2002, enter the following:

```
<4500>display stop-accounting-buffer time-range 0:0:0-2003/08/31
23:59:59-2003/08/31
Total find    0 record
```

key

Syntax

key { accounting | **authentication } *string***

undo key { accounting | **authentication }**

View

RADIUS Scheme View

Parameter

accounting: Configures to set/delete the authentication key for the RADIUS accounting packet.

authentication: Configures to set/delete the encryption key for RADIUS authentication/authorization packet.

string: Specifies the key with a character string not exceeding 16 characters. By default, the key is "3Com".

Description

Use the **key** command to configure encryption key for RADIUS authentication/authorization or accounting packet. Use the **undo key** command to restore the default key.

RADIUS client (Switch) and RADIUS server use MD5 algorithm to hash the exchanged packets. The two ends verify the packet through setting the key. Only when the keys are identical can both ends accept the packets from each other and give responses. So it is necessary to ensure that the keys set on the Switch and the RADIUS server are identical. If the authentication/authorization and accounting are performed on two different servers with different keys, you should set two keys respectively.

Related commands: **primary accounting**, **primary authentication**, **radius scheme**.

Example

Example 1:

To set the authentication/authorization key of the RADIUS scheme to "hello", enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]radius scheme 3Com
[4500-radius-3Com]key authentication hello
```

Example 2:

To set the accounting packet key of the RADIUS scheme to "ok", enter the following:

```
[4500-radius]key accounting ok
```

local-server

Syntax

local-server nas-ip *ip-address* key *string*

undo local-server nas-ip *ip-address*

View

System View

Parameter

nas-ip *ip-address*: set NAS-IP address of access server. ***ip-address*** is expressed in the format of dotted decimal. By default, there is a local server with the NAS-IP address of 127.0.0.1.

key *string*: Set the shared key, **string** is a character string containing up to 16 characters.

Description

Use the **local-server** command to configure the parameters of local RADIUS server. Use the **undo local-server** command to cancel a local RADIUS server.

RADIUS service, which adopts authentication/authorization/accounting servers to manage users, is widely used in the Switch 4500. Besides, local authentication/authorization service is also used in these products and it is called local RADIUS function, that is, realize basic RADIUS function on the Switch.

When using local RADIUS server function, remember the number of the UDP port used for authentication is 1645 and that for accounting is 1646.

The key configured by this command must be the same as that of the RADIUS authentication/authorization packet configured by the command **key authentication** *in the RADIUS Scheme View.*

The Switch 4500 Series supports up to 16 local RADIUS authentication servers.

Related commands: **radius scheme**, **state** and **key**.

Example

To set the IP address of local RADIUS authentication server to 10.110.1.2 and the password to 3Com, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]local-server nas-ip 10.110.1.2 key 3Com
```

nas-ip

Syntax

nas-ip *ip-address*

undo nas-ip

View

RADIUS Scheme View

Parameter

***ip-address*:** IP address in dotted decimal format.

Description

Use the **nas-ip** command to set the source IP address of the network access server (NAS, the Switch in this guide), so that all packets destined for the RADIUS server carry the same source IP address. Use the undo **nas-ip** command to cancel the configuration.

Specifying a source address for the RADIUS packets to be transmitted can avoid the situation where the packets sent back by the RADIUS server cannot be received as the result of a physical interface failure. The address of a loopback interface is usually used as the source address.

By default, the source IP address of packets is the IP address of the output port.

Related commands: **display radius**, **radius nas-ip**.

Example

To set the source IP address that is carried in the RADIUS packets sent by the NAS (the Switch) to 10.1.1.1, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]radius scheme test1
New radius scheme
[4500-radius-test1]nas-ip 10.1.1.1
```

primary accounting

Syntax

primary accounting *ip-address* [*port-number*]

undo primary accounting

View

RADIUS Scheme View

Parameter

ip-address: IP address, in dotted decimal format.

port-number: Specifies UDP port number. ranging from 1 to 65535.

Description

Use the **primary accounting** command to configure the IP address and port number for the primary accounting server. Use the **undo primary accounting** command to restore the default IP address and port number of the primary RADIUS accounting server.

By default, as for the newly created RADIUS scheme, the IP address of the primary accounting server is 0.0.0.0, and the UDP port number of this server is 1813; as for the "system" RADIUS scheme created by the system, the IP address of the primary accounting server is 127.0.0.1, and the UDP port number is 1646. For the newly created RADIUS scheme, the IP address of the primary accounting server is 0.0.0.0 and the UDP port number of this server is 1813.

After creating a RADIUS scheme, you are supposed to set IP addresses and UDP port numbers for the RADIUS servers, including primary/second authentication/authorization servers and accounting servers. In real networking environments, the above parameters shall be set according to the specific requirements. However, you must set at least one authentication/authorization server and an accounting server. Besides, ensure that the RADIUS service port settings on the Switch is consistent with the port settings on the RADIUS server.

Related commands: **key**, **radius scheme**, **state**.

Example

To set the IP address of the primary accounting server of RADIUS scheme, "3Com", to 10.110.1.2 and the UDP port 1813 to provide RADIUS accounting service, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]radius scheme 3Com
[4500-radius-3Com]primary accounting 10.110.1.2 1813
```

primary authentication

Syntax

primary authentication ***ip-address*** **[** ***port-number*** **]**

undo primary authentication

View

RADIUS Server Group View

Parameter

ip-address: IP address, in dotted decimal format. By default, the IP addresses of the primary authentication/authorization is at 0.0.0.0.

port-number: Specifies UDP port number. ranging from 1 to 65535. By default, the UDP port for authentication/authorization service is 1812.

Description

Use the **primary authentication** command to configure the IP address and port number for the primary RADIUS authentication/authorization. Use the **undo primary authentication** command to restore the default IP address and port number of the primary RADIUS authentication/authorization.

By default, for the RADIUS scheme created by the system, the IP address of the primary authentication server is 127.0.0.1 and the UDP port number is 1645. For the newly created RADIUS scheme, the IP address of the primary authentication server is 0.0.0.0 and the UDP port number of this server is 1812.

After creating a RADIUS server group, you are supposed to set IP addresses and UDP port numbers for the RADIUS servers, including primary/second authentication/authorization servers and accounting servers. In real networking environments, the above parameters shall be set according to the specific requirements. However, you set at least one authentication/authorization server and an accounting server. Besides, ensure that the RADIUS service port settings on the Switch is consistent with the port settings on the RADIUS server.

Related commands: **key**, **radius scheme**, **state**.

Example

To set the IP address of the primary authentication/authorization server of RADIUS server group, "3Com", to 10.110.1.1 and the UDP port 1812 to provide RADIUS authentication/authorization service, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]radius scheme 3Com
[4500-radius-3Com]primary authentication auth 10.110.1.1 1812
```

radius nas-ip

Syntax

radius nas-ip ***ip-address***

undo radius nas-ip

View

System View

Parameter

ip-address: IP address in dotted decimal format.

Description

Use the **radius nas-ip** command to specify the source address of the RADIUS packet sent from NAS. Use the **undo radius nas-ip** command to restore the default setting.

By specifying the source address of the RADIUS packet, you can avoid unreachable packets as returned from the server upon interface failure. The source address is normally recommended to be a loopback interface address.

By default, the source address is not specified, that is, the address of the interface sending the packet serves as the source address.

This command specifies only one source address; therefore, the newly configured source address may overwrite the original one.

Example

To configure the Switch to send RADIUS packets from 129.10.10.1, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]radius nas-ip 129.10.10.1
```

radius scheme

Syntax

radius scheme *radius-scheme-name*

undo radius scheme *radius-scheme-name*

View

System View

Parameter

radius-scheme-name: Specifies the Radius server name with a character string not exceeding 32 characters.

Description

Use the **radius scheme** command to configure a RADIUS scheme group and enter its view. Use the **undo radius scheme** command to delete the specified RADIUS scheme.

A default RADIUS scheme named ***system*** has been created in the system. The attributes of ***system*** are all default values.

RADIUS protocol configuration is performed on a per-RADIUS-scheme basis. Every RADIUS scheme shall at least have the specified IP address and UDP port number of the RADIUS authentication/authorization/accounting server and some necessary parameters exchanged with the RADIUS client end (Switch). It is necessary to create the RADIUS scheme and enter its view before performing other RADIUS protocol configurations.

A RADIUS scheme can be used by several ISP domains at the same time. You can configure up to 16 RADIUS schemes, including the default RADIUS scheme named as System.

Although **undo radius scheme** can remove a specified RADIUS scheme, the default one cannot be removed. Note that a scheme currently in use by the online user cannot be removed.

Related commands: **key**, **retry realtime-accounting**, **radius-scheme**, **timer realtime-accounting**, **stop-accounting-buffer enable**, **retry stop-accounting**, **server-type**, **state**, **user-name-format**, **retry**, **display radius**, **display radius statistics**.

Example

To create a RADIUS scheme named "3Com" and enter its view, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]radius scheme 3Com
New Radius scheme
[4500-radius-3Com]
```

reset radius statistics

Syntax

reset radius statistics

View

User View

Parameter

None

Description

Use the reset radius statistics command to clear the statistic information related to the RADIUS protocol.

Related command: **display radius**.

Example

To clear the RADIUS protocol statistics, enter the following:

```
<4500>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

Parameter

radius-scheme *radius-scheme-name:* Configures to delete the stopping accounting requests from the buffer according to the specified RADIUS server name. ***radius-scheme-name*** specifies the RADIUS server name with a character string not exceeding 32 characters.

session-id *session-id:* Configures to delete the stopping accounting requests from the buffer according to the specified session ID. ***session-id*** specifies the session ID with a character string not exceeding 50 characters.

time-range *start-time stop-time:* Configures to delete the stopping accounting requests from the buffer according to the saving time. ***Start-time*** specifies the start time of the saving time range and ***stop-time*** specifies the stop time of the saving time range. The time is expressed in the format hh:mm:ss-yyyy/mm/dd. When this parameter is set, all the stopping accounting requests saved since ***start-time*** to ***stop-time*** will be deleted.

user-name *user-name:* Configures to delete the stopping accounting requests from the buffer according to the username. ***User-name*** specifies the username, a character string not exceeding 32 characters.

Description

Use the **reset stop-accounting-buffer** command to reset the stopping accounting requests, which are saved in the buffer and have not been responded.

By default, after transmitting the stopping accounting requests, if there is no response from the RADIUS server, the Switch will save the packet in the buffer and

retransmit it for several times, which is set through the **retry realtime-accounting** command.

This command is used to delete the stopping accounting requests from the Switch buffer. You can select to delete the packets transmitted to a specified RADIUS server, or according to the session-id or username, or delete the packets transmitted during the specified time-range.

Related commands: **stop-accounting-buffer enable**, **retry stop-accounting**, **display stop-accounting-buffer**.

Example

To delete the stopping accounting requests saved in the system buffer by the user, user0001@marlboro.net, enter the following:

```
[4500]reset stop-accounting-buffer user-name user0001@marlboro.net
```

To delete the stopping accounting requests saved in the system buffer since 0:0:0 to 23:59:59 on August 31, 2002, enter the following:

```
[4500]reset stop-accounting-buffer time-range 0:0:0-2002/08/31
23:59:59-2002/08/31
```

retry

Syntax

retry ***retry-times***

undo retry

View

RADIUS Scheme View

Parameter

retry-times: Specifies the maximum times of retransmission, ranging from 1 to 20. By default, the value is 3.

Description

Use the **retry** command to configure the RADIUS request retransmission times. Use the **undo retry** command to restore the ***retry-times*** to default value.

Because RADIUS protocol uses UDP packets to carry the data, its communication process is not reliable. If the RADIUS server has not responded NAS until timeout, NAS has to retransmit RADIUS request packet. If it transmits more than the specified retry-time, NAS considers that the communication with the current RADIUS server has been disconnected and it will transmit request packet to other RADIUS servers.

Setting a suitable retry-time according to the network situation can speed up the system response.

Related command: **radius scheme**

Example

To set to retransmit the RADIUS request packet no more than 5 times via the server 3Com in the RADIUS scheme, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]radius scheme 3Com
[4500-radius-3Com]retry 5
```

retry realtime-accounting

Syntax

retry realtime-accounting ***retry-times***

undo retry realtime-accounting

View

RADIUS Scheme View

Parameter

retry-times: Specifies the maximum times of real-time accounting request failing to be responded, ranging from 1 to 255. By default, the accounting request can fail to be responded up to 5 times.

Description

Use the **retry realtime-accounting** command to configure the maximum number of retries for real-time accounting requests. Use the **undo retry realtime-accounting** command to restore the maximum number of retries for real-time accounting requests to the default value.

RADIUS server usually checks if a user is online with timeout timer. If the RADIUS server has not received the real-time accounting packet from NAS, it will consider that there is line or device failure and stop accounting. Therefore, it is necessary to disconnect the user at the NAS end and on the RADIUS server synchronously when unexpected failure occurs. The Switch 4500 Series supports a maximum number of times that real-time accounting requests can fail to be responded to. NAS will disconnect the user if it has not received a real-time accounting response from the RADIUS server for the number of specified times.

How is the value of *count* calculated? Suppose RADIUS server connection will timeout in T and the real-time accounting interval of NAS is t, then the integer part of the result from dividing T by t is the value of *count*. Therefore, when applied, T is suggested the numbers which can be divided exactly by t.

Related command: **radius scheme**.

Example

To allow the real-time accounting request failing to be responded for up to 10 times, enter the following:

```
<4500> system-view
System View: return to User View with Ctrl+Z.
[4500]radius scheme 3Com
[4500-radius-3Com]retry realtime-accounting 10
```

retry stop-accounting

Syntax

retry stop-accounting ***retry-times***

undo retry stop-accounting

View

RADIUS Scheme View

Parameter

retry-times: Specifies the maximal retransmission times after stopping accounting request,. ranging from 10 to 65535. By default, the value is 500.

Description

Use the **retry stop-accounting** command to configure the maximal retransmission times after stopping accounting request. Use the **undo retry stop-accounting** command to restore the retransmission times to the default value.

Because the stopping accounting request concerns account balance and will affect the amount of charge, which is very important for both the user and ISP, NAS shall make its best effort to send the message to RADIUS accounting server. Accordingly, if the message from the Switch to RADIUS accounting server has not been responded, the Switch shall save it in the local buffer and retransmit it until the server responds or discard the messages after transmitting for specified times.

Related commands: **reset stop-accounting-buffer**, **radius scheme**, **display stop-accounting-buffer**.

Example

To indicate that, when stopping accounting request for the server "3Com" in the RADIUS server group, the Switch will retransmit the packets for up to 1000 times, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]radius scheme 3Com
[4500-radius-3Com]retry stop-accounting 1000
```

secondary accounting

Syntax

secondary accounting ***ip-address*** **[** ***port-number*** **]**
undo secondary accounting

View

RADIUS Scheme View

Parameter

ip-address: IP address, in dotted decimal format. By default, the IP addresses of second accounting server is at 0.0.0.0.

port-number: Specifies the UDP port number, ranging from 1 to 65535. By default, the accounting service is provided via UDP 1813.

Description

Use the **secondary accounting** command to configure the IP address and port number for the second RADIUS accounting server. Use the **undo secondary accounting** command to restore the IP address and port number to default values.

For detailed information, read the Description of the **primary accounting** command.

Related commands: **key**, **radius scheme**, **state**.

Example

To set the IP address of the second accounting server of RADIUS scheme, 3Com, to 10.110.1.1 and the UDP port 1813 to provide RADIUS accounting service, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]radius scheme 3Com
[4500-radius-3Com]secondary accounting 10.110.1.1 1813
```

secondary authentication

Syntax

secondary authentication ***ip-address*** **[** ***port-number*** **]**

undo secondary authentication

View

RADIUS Scheme View

Parameter

ip-address: IP address, in dotted decimal format. By default, the IP addresses of second authentication/authorization is at 0.0.0.0.

port-number: Specifies the UDP port number, ranging from 1 to 65535. By default, the authentication/authorization service is provided via UDP 1812

Description

Use the **secondary authentication** command to configure the IP address and port number for the second RADIUS authentication/authorization. Use the **undo secondary authentication** command to restore the IP address and port number to default values.

For detailed information, read the Description of the **primary authentication** command.

Related commands: **key**, **radius scheme**, **state**.

Example

To set the IP address of the second authentication/authorization server of RADIUS scheme, "3Com", to 10.110.1.2 and the UDP port 1812 to provide RADIUS authentication/authorization service, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]radius scheme 3Com
[4500-radius-3Com]secondary authentication 10.110.1.2 1812
```

server-type

Syntax

server-type { 3com | **standard }**

undo server-type

View

RADIUS Scheme View

Parameter

3Com: Configures the Switch to support the extended RADIUS server type, which requires the RADIUS client end (Switch) and RADIUS server to interact according RADIUS extensions.

standard: Configures the Switch to support the RADIUS server of Standard type, which requires the RADIUS client end (Switch) and RADIUS server to interact according to the regulation and packet format of standard RADIUS protocol (RFC 2138/2139 or newer).

Description

Use the **server-type** command to configure the RADIUS server type supported by the Switch. Use the **undo server-type** to restore the RADIUS server type to the default value.

By default, the newly created RADIUS scheme supports the server of standard. type, while the "system" RADIUS scheme created by the system supports the server of 3Com type.

The Switch 4500 supports standard RADIUS protocol and the extended RADIUS service platform independently developed by 3Com. This command is used to select the supported RADIUS server type.

Related command: **radius scheme**.

Example

To set the RADIUS server type of RADIUS scheme, "3Com" to 3Com, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]radius scheme 3Com
[4500-radius-3Com]server-type 3Com
```

state

Syntax

state { primary | secondary } { accounting | authentication } { block | active }

View

RADIUS Scheme View

Parameter

primary: Configures to set the state of the primary RADIUS server.

secondary: Configures to set the state of the second RADIUS server.

accounting: Configures to set the state of RADIUS accounting server.

authentication: Configures to set the state of RADIUS authentication/authorization.

block: Configures the RADIUS server to be in the state of **block**.

active: Configures the RADIUS server to be **active**, namely the normal operation state.

Description

Use the **state** command to configure the state of RADIUS server.

By default, as for the newly created RADIUS scheme, the primary and secondary accounting/authentication servers are in the state of **block**; as for the "system" RADIUS scheme created by the system, the primary accounting/authentication servers are in the state of **active**, and the secondary accounting/authentication servers are in the state of **block.**

For the primary and second servers (no matter an authentication/authorization or an accounting server), if the primary server is disconnected to NAS for some fault, NAS will automatically turn to exchange packets with the second server. However, after the primary one recovers, NAS will not resume the communication with it at once, instead, it continues communicating with the second one. When the second one fails to communicate, NAS will turn to the primary one again. This command is used to set the primary server to be **active** manually, in order that NAS can communicate with it right after the troubleshooting.

When the primary and second servers are all **active** or **block**, NAS will send the packets to the primary server only.

Related commands: **radius scheme**, **primary authentication**, **secondary authentication**, **primary accounting**, **secondary accounting**.

Example

To set the second authentication server of RADIUS scheme, "3Com", to be active, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]radius scheme 3Com
[4500-radius-3Com]state secondary authentication active
```

stop-accounting-buffer enable

Syntax

stop-accounting-buffer enable

undo stop-accounting-buffer enable

View

RADIUS Scheme View

Parameter

None

Description

Use the **stop-accounting-buffer enable** command to configure to save the stopping accounting requests without response in the Switch buffer. Use the **undo stop-accounting-buffer enable** command to cancel the function of saving the stopping accounting requests without response in the Switch buffer.

By default, enable to save the stopping accounting requests in the buffer.

Because the stopping accounting request concerns the account balance and will affect the amount of charge, which is very important for both the user and ISP, NAS shall make its best effort to send the message to the RADIUS accounting server. Accordingly, if the message from the Switch to the RADIUS accounting server has not been responded to, the Switch shall save it in the local buffer and retransmit it until the server responds or discard the messages after transmitting for a specified number of times.

Related commands: **reset stop-accounting-buffer**, **radius scheme**, **display stop-accounting-buffer**.

Example

To indicate that, for the server "3Com" in the RADIUS scheme, the Switch will save the stopping accounting request packets in the buffer, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]radius scheme 3Com
[4500-radius-3Com]stop-accounting-buffer enable
```

timer

Syntax

timer ***seconds***

undo timer

View

RADIUS Scheme View

Parameter

seconds: RADIUS server response timeout timer, ranging from 1 to 10 and measured in seconds. By default, the value is 3.

Description

Use the **timer** command to configure RADIUS server response timer. Use the **undo timer** command to restore the default value of the timer.

After a RADIUS (authentication/authorization or accounting) request packet has been transmitted for a period of time, if NAS has not received the response from the RADIUS server, it has to retransmit the message to guarantee RADIUS service for the user. The period taken is called RADIUS server response timeout time, which is controlled by the RADIUS server response timeout timer in the Switch. This command is used to set this timer.

Setting a suitable timer according to the network situation will enhance system performance.

Related commands: **radius scheme**, **retry**.

Example

To set the response timeout timer of RADIUS scheme, 3Com, to 5 seconds, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]radius scheme 3Com
[4500-radius-3Com]timer 5
```

timer quiet

Syntax

time quiet ***minutes***

undo timer quiet

View

RADIUS Scheme View

Parameter

minutes: Quiet time interval, ranging from 1 to 255 in minutes. The default value is 5.

Description

Use the **timer quiet** command to set the quiet time interval after which the primary and secondary RADIUS scheme servers switch over. Use the **undo timer quiet** to set the quiet time interval to its default value.

The functions of the quite time interval are as follows:

1. The Switch sends RADIUS packets to the primary RADIUS server.
2. If the Switch affirms that the primary server does not respond, it then sends RADIUS packets to the secondary RADIUS server.
3. After each quiet time interval, the Switch sets the status of the primary RADIUS server to active and sends RADIUS packets to it next time.

Example

To set the quiet time interval of the RADIUS server group '3Com' to 3 minutes, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z
[4500]radius scheme 3com
[4500-radius-3com]timer quiet 3
```

timer realtime-accounting

Syntax

timer realtime-accounting ***minutes***

undo timer realtime-accounting

View

RADIUS Scheme View

Parameter

minutes: Real-time accounting interval, ranging from 3 to 60, measured in minutes in multiples of 3. By default, the value is 12.

Description

Use the **timer realtime-accounting** command to configure the real-time accounting interval. Use the **undo timer realtime-accounting** command to restore the default interval.

To implement real-time accounting, it is necessary to set a real-time accounting interval. After the attribute is set, NAS will transmit the accounting information of online users to the RADIUS server regularly.

The value of ***minutes*** is related to the performance of NAS and RADIUS server. The smaller the value is, the higher the requirement for NAS and RADIUS server is. When there are a large amount of users (more than 1000, inclusive), we suggest a larger value. The following table recommends the ratio of ***minutes*** value to number of users.

Table 31 Recommended ratio of **minutes** to number of users

Number of users	Real-time accounting interval (minute)
1 to 99	3
100 to 499	6
500 to 999	12
≥1000	≥15

Related commands: **retry realtime-accounting**, **radius scheme**.

Example

To set the real-time accounting interval of RADIUS scheme, "3Com", to 15 minutes, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]radius scheme 3Com
[4500-radius-3Com]timer realtime-accounting 15
```

timer response-timeout

Syntax

timer response-timeout ***seconds***

undo timer response-timeout

View

RADIUS Scheme View

Parameter

***seconds*:** RADIUS server response timeout timer, ranging from 1 to 10 seconds. By default, the value is 3.

Description

Use the **timer response-timeout** command to configure the RADIUS server response timer.

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

If the NAS receives no response from the RADIUS server after sending a RADIUS request (authentication/authorization or accounting request) for a period of time, the NAS resends the request, thus ensuring the user can obtain the RADIUS service. You can specify this period by setting the RADIUS server response timeout timer, taking into consideration the network condition and the desired system performance.

Related commands: **radius scheme**, **retry**.

Example

To set the response timeout timer in the RADIUS scheme 3Com to 5 seconds, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]radius scheme 3Com
[4500-radius-3Com]timer response-timeout 5
```

user-name-format

Syntax

user-name-format { with-domain | without-domain }

View

RADIUS Scheme View

Parameter

with-domain: Specifies to send the username with domain name to RADIUS server.

without-domain: Specifies to send the username without domain name to RADIUS server.

Description

Use the **user-name-format** command to configure the username format sent to RADIUS server.

By default, the username sent to RADIUS servers includes the ISP domain name.

The supplicants are generally named in `userid@isp-name` format. The part following "@" is the ISP domain name. The Switch will put the users into certain ISP domains according to the domain names. However, some earlier RADIUS servers reject the username including the ISP domain name. In this case, the username will be sent to the RADIUS server after its domain name is removed. Accordingly, the Switch provides this command to decide whether the username that is to be sent to RADIUS server carries the ISP domain name or not.

If a RADIUS scheme is configured to reject usernames including ISP domain names, the RADIUS scheme shall not be simultaneously used in more than one ISP

domains. Otherwise, the RADIUS server will regard two users in different ISP domains as the same user by mistake, if they have the same username (excluding their respective domain names.)

Related command: **radius scheme**.

Example

To specify to send the username without domain name to RADIUS server, enter the following:

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]radius scheme 3Com
[4500-radius-3Com]user-name-format without-domain
```

12 USING SYSTEM MANAGEMENT COMMANDS

This chapter describes how to use the following commands:

File System Management Commands

- cd
- copy
- delete
- dir
- execute
- file prompt
- format
- mkdir
- more
- move
- pwd
- rename
- reset recycle-bin
- rmdir
- undelete

Configuration File Management Commands

- display current-configuration
- display saved-configuration
- display this
- display startup
- reset saved-configuration
- save
- startup bootrom-access enable
- startup saved configuration

FTP Server Configuration Commands

- display ftp-server
- display ftp-user
- ftp server

- ftp timeout
- local-user
- password
- service-type

FTP Client Commands

- ascii
- binary
- bye
- cd
- cdup
- close
- delete
- dir
- disconnect
- ftp
- get
- lcd
- ls
- mkdir
- passive
- put
- pwd
- quit
- remotehelp
- rmdir
- user
- verbose

TFTP Configuration Commands

- tftp get
- tftp put

MAC Address Table Management Commands

- display mac-address
- display mac-address aging-time
- mac-address
- mac-address max-mac-count
- mac-address timer

Device Management Commands

- boot boot-loader
- boot bootrom
- display boot-loader
- display cpu
- display device
- display fan
- display memory
- display power
- display schedule reboot
- reboot
- schedule reboot at
- schedule reboot delay

Basic System Configuration and Management Commands

- clock datetime
- clock summer-time
- clock timezone
- sysname

System Status and System Information Display Commands

- display clock
- display config-agent
- display debugging
- display version

System Debug Commands

- debugging
- display diagnostic-information

Network Connection Test Commands

- end-station polling ip-address
- ping
- remote-ping
- display remote-ping
- remote-ping-agent enable
- tracert

Log Commands

- display channel
- display info-center

- info-center channel name
- info-center console channel
- info-center enable
- info-center logbuffer
- info-center loghost
- info-center loghost source
- info-center monitor channel
- info-center snmp channel
- info-center source
- info-center switch-on
- info-center timestamp
- info-center trapbuffer
- reset logbuffer
- reset trapbuffer
- terminal debugging
- terminal logging
- terminal monitor
- terminal trapping

SNMP Configuration Commands

- display snmp-agent
- display snmp-agent community
- display snmp-agent group
- display snmp-agent mib-view
- display snmp-agent statistics
- display snmp-agent sys-info
- display snmp-agent usm-user
- display snmp-proxy unit
- enable snmp trap
- snmp-agent community
- snmp-agent group
- snmp-agent local-engineid
- snmp-agent mib-view
- snmp-agent packet max-size
- snmp-agent sys-info
- snmp-agent target-host
- snmp-agent trap enable
- snmp-agent trap life
- snmp-agent trap queue-size

- snmp-agent trap source
- snmp-agent usm-user
- undo snmp-agent

RMON Configuration Commands

- display rmon alarm
- display rmon event
- display rmon eventlog
- display rmon history
- display rmon prialarm
- display rmon statistics
- rmon alarm
- rmon event
- rmon history
- rmon prialarm
- rmon statistics

NTP Configuration Commands

- display ntp-service sessions
- display ntp-service status
- display ntp-service trace
- ntp-service access
- ntp-service authentication enable
- ntp-service authentication-keyid
- ntp-service broadcast-client
- ntp-service broadcast-server
- ntp-service in-interface disable
- ntp-service max-dynamic-sessions
- ntp-service multicast-client
- ntp-service multicast-server
- ntp-service reliable authentication-keyid
- ntp-service source-interface
- ntp-service unicast-peer

SSH Terminal Service Configuration Commands

- debugging ssh server
- display rsa local-key-pair public
- display rsa peer-public-key
- display ssh server
- display ssh user-information

- peer-public-key end
- protocol inbound
- public-key-code begin
- public-key-code end
- rsa local-key-pair create
- rsa local-key-pair destroy
- rsa peer-public-key
- ssh server authentication-retries
- ssh server timeout
- ssh user assign rsa-key
- ssh user authentication-type

SSH Client Configuration Commands

- display ssh server-info
- peer-public-key end
- public-key-code begin
- public-key-code end
- quit
- rsa peer-public-key
- ssh client assign rsa-key
- ssh client first-time enable
- ssh2

SFTP Server Configuration Commands

- sftp server enable
- ssh user service-type

SFTP Client Configuration Commands

- bye
- cd
- cdup
- delete
- dir
- exit
- get
- help
- ls
- mkdir
- put
- pwd

File System Management Commands

This section describes the commands you can use to manage the file system on your Switch 4500.

In switches supporting the XRN feature, the file path must start with "unit[No.]>flash:/:", the [No.] is the unit ID. For example, suppose unit ID is 1, and the path of the "text.txt" file under the root directory must be "unit1>flash:/text.txt".

cd

Syntax

cd *directory*

View

User view

Parameter

directory: Destination directory. The default directory is the working path configured by the user when the system starts.

Description

Use the **cd** command to change the current user configuration path on the Switch.

Example

Change the current working directory of the switch to flash.

```
<4500>cd flash:
<4500>pwd
unit1>flash:
<4500>
```

copy

Syntax

copy *filepath-source filepath-dest*

View

User view

Parameter

filepath-source: Source file name.

filepath-dest: Destination file name.

Description

Use the **copy** command to copy a file.

When the destination filename is the same as that of an existing file, the system will ask whether to overwrite it.

Example

Display current directory information.

```
<4500>dir
Directory of unit1>flash:/
0   -rw-       595  Jul 12 2001 19:41:50   test.txt
16125952 bytes total (13975552 bytes free)
```

Copy the file test.txt and save it as test.bak.

```
<4500>copy test.txt test.bak
%Copy file unit1>flash:/test.txt to unit1>flash:/test.bak
...Done
```

Display current directory information.

```
<4500>dir
Directory of unit1>flash:/
   0   -rw-       595  Jul 12 2001 19:41:50   test.txt
   1   -rw-       595  Jul 12 2001 19:46:50   test.bak
16125952 bytes total (13974528 bytes free)
```

delete

Syntax

delete [/ unreserved] ***file-path***

View

User view

Parameter

/unreserved: The file will be deleted permanently if the user chooses this parameter

file-path: Path and name of the file you want to delete.

Description

Use the **delete** command to delete a specified file from the storage device of the Switch.

The deleted files are kept in the recycle bin and will not be displayed when you use the **dir** command. However they will be displayed, using the **dir /all** command. The files deleted by the **delete** command can be recovered with the **undelete** command or deleted permanently from the recycle bin, using the **reset recycle-bin** command.

If two files with the same name in a directory are deleted, only the latest deleted file will be kept in the recycle bin.

Example

Delete the file flash:/test/test.txt

```
<4500>delete flash:/test/test.txt
Delete unit1>flash:/test/test.txt?[Y/N]:y
%Delete file unit1>flash:/test/test.txt...Done.
```

```
<4500>
```

dir

Syntax

dir [/all] [*file-path*]

View

User view

Parameter

/all: Display all the files (including the deleted ones).

file-path: File or directory name to be displayed. The ***file-path*** parameter supports "*" matching. For example, using **dir *.txt** will display all the files with the extension **txt** in the current directory.

dir without any parameters will display the file information in the current directory.

Description

Use the **dir** command to display the information about the specified file or directory in the storage device of the Switch.

Example

Display the information for file flash:/test/test.txt

```
<4500>dir flash:/test/test.txt
Directory of unit1>flash:/test/test.txt
1 -rw-    248     Aug 29 2000 17:49:36 text.txt
20578304 bytes total (3104544 bytes free)
```

Display information for directory flash:/test/

```
<4500>dir flash:/test/
Directory of unit1>flash:/test/
1 -rw-  248  Aug 29 2000 17:49:36 test.txt
20578304 bytes total (3104544 bytes free)
```

Display all of the files with names starting with "t" in directory flash:/test/

```
<4500>dir flash:/test/t*
Directory of unit1>flash:/test/t*
1 -rw-  248  Aug 29 2000 17:49:36 test.txt
20578304 bytes total (3104544 bytes free)
```

Display information about all of the files (including the deleted files) in directory flash:/test/

```
<4500>dir /all flash:/test/
Directory of unit1>flash:/test/
1 -rw-  248     Aug 29 2000 17:49:36 text.txt
20578304 bytes total (3104544 bytes free)
```

Display information about all of the files (including the deleted files) with names starting with "t" in flash:/test/

```
<4500>dir /all flash:/test/t*
Directory of unit1>flash:/test/t*
```

```
1 -rw-  248     Aug 29 2000 17:49:36 text.txt
20578304 bytes total (3104544 bytes free)
```

execute

Syntax

execute *filename*

View

System view

Parameter

filename: Name of the batch file, which is a string up to 256 characters in length, with a suffix of ".bat".

Description

Use the **execute** command to execute the specified batch file.

The batch command executes the command lines in the batch file one by one. There should be no invisible character in the batch file. If invisible characters are found, the batch command will quit the current execution. The forms and contents of the commands are not restricted in the batch file.

Example

To execute the batch file "test.bat" in the directory of "flash:/", enter the following:

```
<4500>sys
System View: return to User View with Ctrl+Z.
[4500]execute test.bat
```

file prompt

Syntax

file prompt { alert | quiet }

View

System view

Parameter

alert: Select confirmation on dangerous file operations.; the default value is alert.

quiet: No confirmation prompt on file operations.

Description

Use the **file prompt** command to modify the prompt mode of file operations on the Switch.

If the prompt mode is set as **quiet**, so no prompts are shown for file operations, some non-recoverable operations may lead to system damage.

Example

Configure the prompt mode of file operation as **quiet**.

```
<4500>sys
System View: return to User View with Ctrl+Z
```

```
[4500]file prompt quiet
[4500]
```

format

Syntax

format *filesystem*

View

User view

Parameter

filesystem: Device name.

Description

Use the **format** command to format the storage device. All of the files on the storage device will be lost and non-recoverable. Specially, configuration files will be lost after formatting flash memory.

Example

Format flash:

```
<4500>format unit1>flash:
All data on unit1>flash: will be lost , proceed with format ? [Y/N] y
% Now begin to format flash, please wait for a while...
Format unit1>flash: completed
```

mkdir

Syntax

mkdir *directory*

View

User view

Parameter

directory: Directory name.

Description

Use the **mkdir** command to create a directory in the specified directory on the storage device.

The directory to be created cannot have the same name as that of any other directory or file in the specified directory.

Example

Create the directory dd.

```
<4500>mkdir dd
Created dir unit1>flash:dd
<4500>
```

more

Syntax

more ***file-path***

View

User view

Parameter

file-path: File name.

Description

Use the **more** command to display the contents f of the specified file formatted as text.

Example

Display contents of file test.txt.

```
<4500>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.
<4500>
```

move

Syntax

move *filepath-source filepath-dest*

View

User view

Parameter

filepath-source: Source file name.

filepath-dest: Destination file name.

Description

Use the **move** command to move files.

When the destination filename is the same as that of an existing file, the system will ask whether to overwrite the existing file.

Example

Display the current directory information.

```
<4500>dir
Directory of unit1>flash:/
   0   -rw-   2145718  Jul 12 2001 12:28:08   ne80.bin
   1   drw-         0  Jul 12 2001 19:41:20   test
16125952 bytes total (13970432 bytes free)

<4500>dir unit1>flash:/test/
Directory of unit1>flash:/test/
   0   drw-         0  Jul 12 2001 20:23:37   subdir
   1   -rw-        50  Jul 12 2001 20:08:32   sample.txt
16125952 bytes total (13970432 bytes free)
```

Move flash:/test/sample.txt to flash:/sample.txt.

```
<4500>move flash:/test/sample.txt flash:/sample.txt
Move unit1>flash:/test/sample.txt to unit1>flash:/sample.txt
?[confirm]:y
% Moved file unit1>flash:/test/sample.txt unit1>flash:/sample.txt
```

Display the directory after moving a file.

```
<4500>dir
Directory of unit1>flash:/
   0   -rw- 2145718  Jul 12 2001 12:28:08   3Com.bin
   1   drw-         0  Jul 12 2001 19:41:20   test
   2   -rw-        50  Jul 12 2001 20:26:48   sample.txt
16125952 bytes total (13970432 bytes free)
<4500>dir flash:/test/
Directory of unit1>flash:/test/
   0   drw-         0  Jul 12 2001 20:23:37   subdir
   16125952 bytes total (13970432 bytes free)
```

pwd

Syntax

pwd

View

User view

Parameter

None

Description

Use the **pwd** command to display the current path.

Example

Display the current path.

```
<4500>pwd
unit1>flash:
<4500>
```

rename

Syntax

rename ***filepath-source filepath-dest***

View

User view

Parameter

filepath-source: Source file name.

filepath-dest: Destination file name.

Description

Use the **rename** command to rename a file.

If the destination file name is the same as an existing directory name, the rename operation will fail. If the destination file name is the same as an existing file name, a prompt will be displayed asking whether to overwrite the existing file.

Example

Display the current directory information.

```
<4500>dir
Directory of unit1>flash:
   0 drw-         0  Jul 12 2001 19:41:20   test
   1 -rw-        50  Jul 12 2001 20:26:48   sample.txt
16125952 bytes total (13970432 bytes free)
```

Rename the file sample.txt with sample.bak.

```
<4500>rename sample.txt sample.bak
Rename flash:/sample.txt to flash:/sample.bak ?[confirm]:y
% Renamed file unit1>flash:/sample.txt unit1>flash:/sample.bak
```

Display the directory after renaming sample.txt with sample.bak.

```
<4500>dir
Directory of unit1>flash:
   0   -rw-   2145718  Jul 12 2001 12:28:08   ne80.bin
   1   drw-         0  Jul 12 2001 19:41:20   test
   2   -rw-        50  Jul 12 2001 20:29:55   sample.bak
16125952 bytes total (13970432 bytes free)
```

reset recycle-bin

Syntax

reset recycle-bin *file-path*

View

User view

Parameter

file-path: Name of the file to be deleted.

Description

Use the **reset recycle-bin** command to permanently delete files from the recycle bin.

The **delete** command only puts the file into the recycle bin, but the **reset recycle-bin** command will delete this file permanently.

Example

Delete the file from the recycle bin.

```
<4500>reset recycle-binflash:/plh_logic.out
Clear unit1>flash:/plh_logic.out? [Y/N]:y
Clearing files from flash may take a long time. Please wait.
%Cleared file unit1>flash:/~/ plh_logic.out.
```

rmdir

Syntax

rmdir *directory*

View

User view

Parameter

directory: Directory name.

Description

Use the **rmdir** command to delete a directory. The directory to be deleted must be empty.

Example

Delete the directory **test**.

```
<4500>rmdir test
Rmdir unit1>flash:/test?[Y/N]:y
Removed directory unit1>flash:/test
```

undelete

Syntax

undelete *file-path*

View

User view

Parameter

file-path: Name of the file to be recovered.

Description

Use the **undelete** command to recover the deleted file.

The file name to be recovered cannot be the same as an existing directory name. If the destination file name is the same as an existing file name, a prompt will be displayed asking whether to overwrite the existing file.

Example

Display the information for all of the files in the current directory, including the deleted files.

```
<4500>dir /all
Directory of unit1>flash:/
   0   -rw-       595  Jul 12 2001 20:13:19   test.txt
   1   -rw-        50  Jul 12 2001 20:09:23   [sample.bak]
16125952 bytes total (13972480 bytes free)
```

Recover the deleted file `sample.bak`.

```
<4500>undelete sample.bak
Undelete unit1>flash:/sample.bak ?[confirm]:y
% Undeleted file unit1>flash:/sample.bak
```

Display the information for all of the files in the current directory, including the deleted files .

```
<4500>dir /all
Directory of unit1>flash:/
   0   -rw-        50  Jul 12 2001 20:34:19   sample.bak
   1   -rw-       595  Jul 12 2001 20:13:19   test.txt
16125952 bytes total (13972480 bytes free)
```

Configuration File Management Commands

This section describes the commands you can use to manage the configuration files on your Switch 4500.

display current-configuration

Syntax

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

View

All views

Parameter

controller: View the configuration information of controllers.

interface: View the configuration information of interfaces.

***interface-type*:** Type of the interface.

***interface-number*:** Number of the interface.

configuration ***configuration*:** View specific parts of the current configuration. The value of ***configuration*** is the key word of the configuration, such as:

- **acl-adv:** View the configuration information of advanced ACL.
- **ospf:** View the configuration information of OSPF.
- **system:** View the configuration information of sysname.
- **timerange:** View the configuration information of time range.
- **user-interface:** View the configuration information of user-interface.

|: Filter the configuration information to be output via regular expression.

begin: Begin with the line that matches the regular expression.

exclude: Exclude lines that match the regular expression.

include: Include lines that match the regular expression.

***regular-expression*:** Define the regular expression.

Description

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

By default, if some running configuration parameters are the same with the default operational parameters, they will not be displayed.

If a user needs to authenticate whether the configurations are correct after finishing a set of configuration, the **display current-configuration** command can be used to display the running parameters. Although the user has configured some parameters, but the related functions are not effective, they are not displayed.

When there is much configuration information to use the regular expression to filter the output information. For specific rules about the regular expression, refer to the Switch 4500 Configuration Guide.

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

Example

To view the running configuration parameters of the switch, enter the following:

```
<4500>display current-configuration
local-server nas-ip 127.0.0.1 key 3com
domain default enable system
queue-scheduler wrr 1 2 3 4 5 9 13 15
ip http acl 2000
radius scheme system
domain system
acl number 2000 match-order auto
 rule 0 permit
acl number 3000
acl number 4000
rule 0 permit
qos-profile student
 packet-filter inbound ip-group 2000 rule 0
  ---- More ----
```

To view the lines containing the character string "10*" in the configuration information, enter the following. The "*" indicates that the "0" before it can appear 0 times or multiple consecutive times.

```
<4500>display current-configuration | include 10*
local-server nas-ip 127.0.0.1 key 3com
queue-scheduler wrr 1 2 3 4 5 9 13 15
 traffic-limit inbound ip-group 2000 rule 0 128 exceed drop
vlan 1
 ip address 1.1.1.2 255.255.255.0
interface Aux1/0/0
interface Ethernet1/0/1
 webcache address 1.1.1.1 mac 00e0-fc01-0101 vlan 40
 traffic-limit inbound ip-group 2000 rule 0 128
traffic-redirect inbound ip-group 2000 rule 0 interface
Ethernet1/0/1
line-rate inbound 128
 queue-scheduler wrr 1 2 3 4 5 6 7 8
interface Ethernet1/0/2
interface Ethernet1/0/3
interface Ethernet1/0/4
interface Ethernet1/0/5
```

```
interface Ethernet1/0/6
interface Ethernet1/0/7
interface Ethernet1/0/8
interface Ethernet1/0/9
interface Ethernet1/0/10
interface Ethernet1/0/11
interface Ethernet1/0/12
  ---- More ----
```

To view configuration information beginning with "user", enter the following:

```
<4500>display current-configuration | include ^user
user-interface aux 0 7
user-interface vty 0 4
```

To view the pre-positive and post-positive configuration information, enter the following:

```
<4500>display current-configuration configuration
local-server nas-ip 127.0.0.1 key 3com
domain default enable system
queue-scheduler wrr 1 2 3 4 5 9 13 15
ip http acl 2000
radius scheme system
domain system
acl number 2000 match-order auto
 rule 0 permit
acl number 3000
acl number 4000
 rule 0 permit
qos-profile student
 packet-filter inbound ip-group 2000 rule 0
  ---- More ----
```

display saved-configuration

Syntax

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

View

All views

Parameter

unit *unit-id*: Specify the Unit ID of switch.

Description

Use the **display saved-configuration** command to view the configuration files in the flash memory of the Switch.

If the Switch works abnormally after power on, execute the **display saved-configuration** command to view the startup configuration of the Switch.

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

Example

To display configuration files in flash memory of the Switch, enter the following:

```
<4500>display saved-configuration
local-server nas-ip 127.0.0.1 key 3com
 domain default enable system
 queue-scheduler wrr 1 2 3 4 5 9 13 15
 ip http acl 2000
radius scheme system
domain system
acl number 2000 match-order auto
 rule 0 permit
acl number 3000
acl number 4000
 rule 0 permit
qos-profile student
  ---- More ----
```

display this

Syntax

display this

View

All views

Parameter

None

Description

Use the **display this** command, to display the configuration of the current view. If you need to authenticate whether the configurations are correct, after you have finished a set of configurations under a view to use the **display this** command to view the parameters.

Some effective parameters are not displayed if they are the same as the default ones. Some ineffective parameters that were configured by the user, are not displayed either.

Associated configuration of the interface is displayed when executing the command in different interface views, related configuration of the protocol view is displayed when excecuting this command in different protocol views, and all the configurations of the protocol views are displayed when executing this command in protocol sub-views.

For the related command, see **save, reset, saved-configuration, display current-configuration, display saved-configuration**.

Example

Display the configuration parameters for the current view of the switch system.

```
<4500>sys
System View: return to User View with Ctrl+Z.
[4500]display this
return
[4500]
```

display startup

Syntax

display startup

View

All views

Parameter

None

Description

Use the **display startup** command, to display the related system software and configuration filenames used for the current and the next start-ups.

This command is used to display the following information:

- Filename of the system software configured by the user
- Filename of the system software actually used for this startup
- Filename of the system software configured for the next startup
- Configuration filename used for the current startup
- Configuration filename configured for the next startup.

For the related command, see **startup saved-configuration**.

Example

Display the filenames related to the current and the next enabling.

```
<4500>display startup

UNIT1:
  Startup saved-configuration file:          flash:/4500cfg.cfg
  Next startup saved-configuration file:     flash:/4500cfg.cfg
  Bootrom-access enable state:               enabled
```

reset saved-configuration

Syntax

reset saved-configuration

View

User view

Parameter

None

Description

Use the **reset saved-configuration** command to erase configuration files from the flash memory of the Switch.

Consult with technical support personnel before executing this command.

Generally, this command is used in the following situations:

- After upgrade of software, configuration files in flash memory may not match the new version's software. Perform **reset saved-configuration** command to erase the old configuration files.
- When a Switch 4500 is reused on a network but in a different manner to previously, the original configuration file should be erased and the switch reconfigured.

If the configuration files do not exist in the flash memory when the Switch is powered on and initialized, it will choose the default setting automatically.

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

Example

Erase the configuration files from the flash memory of the Switch.

```
<4500>reset saved-configuration
The saved configuration will be erased.
Are you sure?[Y/N]y
Configuration in flash memory is being cleared.
Please wait ...
..
Configuration in flash memory is cleared.
<4500>
```

save

Syntax

save [***filename*** | **safely]**

View

Any view

Parameter

file-name: the name of the configuration file. It is a character string of 5 to 56 characters.

safely: save the configuration file in safely mode.

Description

Use the **save** command, to save the current configuration files to flash memory.

After finishing a group of configurations and achieving corresponding functions, get the current configuration files stored in the flash memory.

After a fabric is formed, if you execute the save command, every switch in the fabric saves the current configurations to its individual configuration file.

If you do not enter the file-name parameter in this command, for the switches that have specified the configuration file for booting by startup saved-configuration command, the current configurations will be stored to the specified configuration file; and for the switches that have not specified the configuration file for booting, the current configurations will be stored to the default configuration file, 4500cfg.cfg.

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

Example

Get the current configuration files stored in flash memory.

```
<4500>save
The configuration will be written to the device.
Are you sure?[Y/N] y
Please input the file name(*.cfg)[flash:/4500cfg.cfg]:
Now saving current configuration to the device.
Saving configuration. Please wait .....
.........
Configuration is saved to flash memory successfully.
 Unit1 save configuration flash:/4500cfg.cfg successfully
<4500>
%Apr  2 01:22:58:141 2000 3Com CFM/3/CFM_LOG:- 1 -Unit1 save
configuration successfully.
```

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 enable the BOOTROM access function.

Use the **undo startup bootrom-access** enable command to disable the BOOTROM access functi

on.

Example

To enable BOOTROM access function, enter the following:

```
<4500>startup bootrom-access enable
```

startup saved configuration

Syntax

startup saved-configuration *cfgfile*

View

User view

Parameter

cfgfile: The name of the configuration file. It is a string with a length of 5 to 56 characters.

Description

Use the **startup saved-configuration** command to configure the configuration file used for enabling the system for the next time.

The configuration file must have ".cfg" as its extension name and must be saved under the root directory of the Flash.

For the related command, please see **display startup**

Example

Configure the configuration file for the next start-up.

```
<4500>startup saved-configuration 4500cfg.cfg
Please wait.............Done!
<4500>
%Apr  2 01:24:57:661 2000 3Com CFM/3/CFM_LOG:- 1 -Unit1 set the
configuration successfully.
```

FTP Server Configuration Commands

This section describes how to use the File Transfer Protocol (FTP) configuration commands on your Switch 4500.

display ftp-server

Syntax

display ftp-server

View

All views

Parameter

None

Description

Use the **display ftp-server** command to display the parameters of the current FTP Server. You can perform this command to verify the configuration after setting FTP parameters.

Example

Display the configuration of FTP Server parameters.

```
<4500>display ftp-server
   Ftp server is running
   Max user number       1
   User count            0
   Timeout(minute)       30
<4500>
```

display ftp-user

Syntax

display ftp-user

View

All views

Parameter

None

Description

Use the **display ftp-user** command to display the parameters of current FTP user. You can perform this command to examine the configuration after setting FTP parameters.

Example

Show the configuration of FTP user parameters.

```
<4500>display ftp-user
% No ftp user
<4500>
```

ftp server

Syntax

```
ftp server enable
undo ftp server
```

View

System view

Parameter

enable: Start FTP Server.

Description

- Use the **ftp server** command to start FTP Server and enable FTP user logon.
- Use the **undo ftp server** command to close FTP Server and disable FTP user logon.

By default, FTP Server is shut down.

Perform this command to easily start or shut down FTP Server, preventing the Switch from being attacked by an unknown user.

Example

Shut down FTP Server.

```
<4500>sys
System View: return to User View with Ctrl+Z.
[4500]undo ftp server
% Close FTP server
[4500]
```

ftp timeout

Syntax

```
ftp timeout minute
undo ftp timeout
```

View

System view

Parameter

minute: Connection timeouts (measured in minutes), ranging from 1 to 35791; The default connection timeout time is 30 minutes.

Description

- Use the **ftp timeout** command to configure connection timeout interval.
- Use the **undo ftp timeout** command to restore the default connection timeout interval.

After a user logs on to an FTP Server and has established connection, if the connection is interrupted or cut abnormally by the user, FTP Server will still hold the connection. The connection timeout can avoid this problem. If the FTP server has no command interaction with a client for a specific period of time, it considers the connection to have failed and disconnects the client.

Example

Set the connection timeout to 36 minutes.

```
<4500>sys
System View: return to User View with Ctrl+Z.
[4500]ftp timeout 36
[4500]
```

local-user

Syntax

local-user *user_name*

undo local-user { *user_name* | all [service-type { telnet | ftp | lan-access | ssh | terminal }] }

View

System view

Parameter

user_name*:** Enter a local user name, up to 80 characters in length, excluding "/", ":", "*", "?", "<" and ">". (The @ character can be used once in a ***user_name; that part of the user name which precedes the @ symbol must not be more than 55 characters in length. The user-name is case-insensitive, so that UserA is the same as usera.

all: Specifies all users.

service-type: Specifies the service type, which can be one of the following:

telnet: Specifies the user type of Telnet.

ftp: Specifies the user type of FTP.

lan-access: Specifies the user type of LAN access, which mainly refers to Ethernet-accessing users.

ssh:Specifies that the user type is SSH.

terminal: Specifies that the user type is terminal which refers to users who use the terminal service (login from the Console, AUX or Asyn port).

Description

Use the **local-user** command to configure a local user and enter the local user view.

Use the **undo local-user** command to cancel a specified local user, a type of user or all users. By default, a local user is not configured.

Related commands: **display local-user**, **service-type**.

Example

To add a local user named 3Com1, enter the following:

```
<4500>sys
System View: return to User View with Ctrl+Z.
[4500]local-user 3Com1
New local user added
[4500-luser-3Com1]
```

password

Syntax

password {simple | **cipher }** ***password***

undo password

View

Local user view

Parameters

simple: Specifies that passwords are displayed in simple text.

cipher: Specifies that passwords are displayed in cipher text.

password: Enter a password, up to 16 characters in length for simple text, and up to 24 characters in length for cipher text.

Description

- Use the **password** command to configure the password display mode for local users.
- Use the **undo password** command to cancel the specified password display mode.

The settings in the **local-user password-display-mode cipher-force***, command override the settings in the* **password** *command.*

Related command: **display local-user**

Example

To set the user 3Com1 to display the password 20030422 in simple text, enter the following:

```
<4500>sys
System View: return to User View with Ctrl+Z.
```

```
[4500]local-user 3Com1
New local user added
[4500-luser-3Com1]password simple 20030422
```

service-type

Syntax

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

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

View

Local user view

Parameters

telnet: Specifies the user's service type as Telnet.

ssh: Specifies the user type as SSH.

level *level*: Specifies the level of Telnet, SSH or terminal users. The argument level is an integer in the range of 0 to 3 and defaults to 1.

ftp: Specifies the user's service type as FTP.

ftp-directory *directory*: Enter an FTP directory, up to 64 characters in length. Optional.

lan-access: Specifies user type to lan-access, which mainly refers to Ethernet accessing users, 802.1x supplicants for example.

terminal: Authorizes the user to use the terminal service (login from the Console, AUX or Asyn port).

Description

Use the **service-type** command to configure a service type for a particular user.

Use the **undo service-type** command to cancel the currently configured service type for a particular user.

If configuring service types: SSH, Telnet or Terminal:

When you configure a new service type for a user, the system adds the new service type to the existing one.

You can set user level when you configure a service type. If you set multiple service types and specify the user levels, then only the last configured user level is valid. Different service type does not have its individual user level.

You can use either **level** *or* **service-type** *command to specify the level for a local user. If both of these two commands are used, the latest configuration will take effect.*

Example

To configure a service type of LAN access for the user 3Com1, enter the following:

```
<4500>sys
System View: return to User View with Ctrl+Z.
[4500]local-user-3Com1
New local user added.
[4500-luser-3Com1]service-type lan-access
```

FTP Client Commands

This section describes the File Transfer Protocol (FTP) Client commands on your Switch 4500.

ascii

Syntax

ascii

View

FTP Client view

Parameter

None

Description

Use the **ascii** command to configure data transmission mode as ASCII mode.

By default, the file transmission mode is ASCII mode.

Perform this command if the user needs to change the file transmission mode to default mode.

Example

Configure to transmit data in the ASCII mode.

```
<4500>ftp 1.1.1.1
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]ascii
200 Type set to A.
[ftp]
```

binary

Syntax

binary

View

FTP Client view

Parameter

None

Description

Use the **binary** command to configure file transmission type as binary mode.

Example

Configure to transmit data in the binary mode.

```
<4500>ftp 1.1.1.1
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]binary
200 Type set to I.
[ftp]
```

bye

Syntax

bye

View

FTP Client view

Parameter

None

Description

Use the **bye** command to disconnect with the remote FTP Server and return to user view.

After performing this command, you can terminate the control connection and data connection with the remote FTP Server.

Example

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

```
<4500>ftp 1.1.1.1
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]bye
221 Server closing.
<4500>
```

cd

Syntax

cd *pathname*

View

FTP Client view

Parameter

pathname: Path name.

Description

Use the **cd** command to change the working path on the remote FTP Server.

This command is used to access another directory on FTP Server. Note that the user can only access the directories authorized by the FTP server.

Example

Change the working path to flash:/temp

```
<4500>ftp 1.1.1.1
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]cd flash:/temp
250 CWD command successful.
[ftp]
```

cdup

Syntax

cdup

View

FTP Client view

Parameter

None

Description

Use the **cdup** command to change working path to the upper level directory.

This command is used to exit the current directory and return to the upper level directory.

Example

Change working path to the upper level directory

```
<4500>ftp 1.1.1.1
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]cdup
501 Change to no authenticated directory.
[ftp]
```

close

Syntax

close

View

FTP Client view

Parameter

None

Description

Use the **close** command to disconnect FTP client side from FTP server side without exiting FTP client side view so that you terminate the control connection and data connection with the remote FTP server at the same time.

Example

Terminate connection with the remote FTP Server and stay in FTP Client view.

```
<4500>ftp 1.1.1.1
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]close
221 Server closing.
[ftp]
```

delete

Syntax

delete remotefile

View

FTP Client view

Parameter

remotefile: File name.

Description

Use the **delete** command to delete the specified file.

This command is used to delete a file.

Example

Delete the file `temp.c`

```
<SW4500>ftp 1.1.1.1
```

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

dir

Syntax

dir [*filename* [*localfile*]]

View

FTP Client view

Parameter

***filename*:** File name to be queried.

***localfile*:** Saved local file name.

Description

Use the **dir** command to query a specified file.

If no parameter of this command is specified, then all the files in the directory will be displayed.

Example

Query the file `temp.c` and save the results in the file `temp1`.

```
<SW4500>ftp 1.1.1.1
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]dir temp.c temp1
200 Port command okay.
150 Opening ASCII mode data connection for temp.c.
....226 Transfer complete.
FTP: 63 byte(s) received in 6.700 second(s) 9.00 byte(s)/sec.
[ftp]
```

disconnect

Syntax

disconnect

View

FTP Client view

Parameter

None

Description

Using the **disconnect** command, subscribers can disconnect FTP client side from FTP server side without exiting FTP client side view.

This command terminates the control connection and data connection with the remote FTP Server at the same time.

Example

Terminate connection with the remote FTP Server and stay in FTP Client view.

```
<SW4500>ftp 1.1.1.1
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]disconnect
221 Server closing
[ftp]
```

ftp

Syntax

ftp [*ipaddress* [*port*]]

View

User view

Parameter

ipaddress: IP address of the remote FTP Server.

port: Port number of remote FTP Server.

Description

Use the **ftp** command to establish control connection with the remote FTP Server and enter FTP Client view.

Example

Connect to FTP Server at the IP address `1.1.1.1`

```
<SW4500>ftp 1.1.1.1
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]
```

get

Syntax

get *remotefile* [*localfile*]

View

FTP Client view

Parameter

localfile: Local file name.

remotefile: Name of a file on the remote FTP Server.

Description

Use the **get** command to download a remote file and save it locally.

If no local file name is specified, it will be considered the same as that on the remote FTP Server.

Example

Download the file `temp1.c` and saves it as `temp.c`

```
<SW4500>ftp 1.1.1.1
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]get temp1.c temp.c
200 Port command okay.
150 Opening ASCII mode data connection for temp1.c.
..226 Transfer complete.
FTP: 1709 byte(s) received in 2.176 second(s) 0.00 byte(s)/sec.
[ftp]
```

lcd

Syntax

lcd

View

FTP Client view

Parameter

None

Description

Use the **lcd** command to display local working path of FTP Client.

Example

Show local working path.

```
<SW4500>ftp 1.1.1.1
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]lcd
% Local directory now flash:/temp
[ftp]
```

ls

Syntax

ls [*remotefile* [*localfile*]]

View

FTP Client view

Parameter

remotefile: Remote file to be queried.

localfile: Saved local file name.

Description

Use the **ls** command to query a specified file.

If no parameter is specified, all the files will be shown.

Example

Query file temp.c

```
<SW4500>ftp 1.1.1.1
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]ls temp.c
200 Port command okay.
150 Opening ASCII mode data connection for temp.c.
temp.c
226 Transfer complete.
FTP: 8 byte(s) received in 0.133 second(s) 60.00byte(s)/sec.
[ftp]
```

mkdir

Syntax

mkdir *pathname*

View

FTP Client view

Parameter

pathname: Directory name.

Description

Use the **mkdir** command to create a directory on the remote FTP Server.

User can perform this operation as long as the remote FTP server has authorized the operation.

Example

Create the directory `flash:/lanswitch` on the remote FTP Server.

```
<SW4500>ftp 1.1.1.1
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]mkdir flash:/lanswitch
257 "flash:/lanswitch" new directory created.
[ftp]
```

passive

Syntax

passive

undo passive

View

FTP Client view

Parameter

None

Description

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

By default, the data transmission mode is passive mode

Example

Set the data transmission to passive mode.

```
<SW4500>ftp 1.1.1.1
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]passive
% Passive is on
[ftp]
```

put

Syntax

put *localfile* [*remotefile*]

View

FTP Client view

Parameter

localfile: Local file name.

remotefile: File name on the remote FTP Server.

Description

Use the **put** command to upload a local file to the remote FTP Server.

If the user does not specify the filename on the remote server, the system will consider it the same as the local file name by default.

Example

Upload the local file `temp.c` to the remote FTP Server and saves it as `temp1.c`.

```
<SW4500>ftp 1.1.1.1
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]put temp.c temp1.c
200 Port command okay.
150 Opening ASCII mode data connection for temp1.c.
226 Transfer complete.
FTP: 1709 byte(s) sent in 0.316 second(s) 5.00Kbyte(s)/sec.
[ftp]
```

pwd

Syntax

pwd

View

FTP Client view

Parameter

None

Description

Use the **pwd** command to display the current directory on the remote FTP Server.

Example

Show the current directory on the remote FTP Server.

```
<SW4500>ftp 1.1.1.1
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]pwd
257 "flash:/temp" is current directory.
[ftp]
```

quit

Syntax

quit

View

FTP Client view

Parameter

None

Description

Use the **quit** command to terminate the connection with the remote FTP Server and return to user view.

Example

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

```
<SW4500>ftp 1.1.1.1
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]quit
221 server closing
<SW5500>
```

remotehelp

Syntax

remotehelp [*protocol-command* **]**

View

FTP Client view

Parameter

protocol-command: FTP protocol command.

Description

Use the **remotehelp** command to display help information about the FTP protocol command.

Example

Show the syntax of the protocol command `user`.

```
<SW5500>ftp 1.1.1.1
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]remotehelp user
214 Syntax: USER <sp> <username>
[ftp]
```

rmdir

Syntax

rmdir *pathname*

View

FTP Client view

Parameter

pathname: Directory name of remote FTP Server.

Description

Use the **rmdir** command to delete the specified directory from FTP Server.

Example

Delete the directory `flash:/temp1` from FTP Server.

```
<SW4500>ftp 1.1.1.1
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]rmdir flash:/temp1
200 RMD command successful.
[ftp]
```

user

Syntax

user *username* [*password*]

View

FTP Client view

Parameter

username: Logon username.

password: Logon password.

Description

Use the **user** command to register an FTP user.

Example

Log in the FTP Server with username `tom` and password `hello`.

```
<SW4500>ftp 1.1.1.1
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]user tom hello
331 Password required for tom.
230 User logged in.
[ftp]
```

verbose

Syntax

verbose

undo verbose

View

FTP Client view

Parameter

None

Description

Use the **verbose** command to enable verbose. Use the **undo verbose** command to disable verbose.

By default, verbose is disabled.

Example

Enable verbose.

```
<SW4500>ftp 1.1.1.1
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]verbose
```

```
% Verbose is on
[ftp]
```

TFTP Configuration Commands

This section describes the Trivial File Transfer Protocol (TFTP) Commands on your Switch 4500.

tftp get

Syntax

tftp *tftpserver* get *source-file* [*dest-file*]

View

User view

Parameter

tftp-server: IP address or host name of the TFTP server. The name of the TFTP server should be a string ranging from 1 to 20 characters.

source-file: Specify the filename of the source file on the TFTP server.

dest-file: Specify the filename of the destination file which will be saved on the switch.

Description

Use the **tftp get** command to download a file from the specified directory of the TFTP server and save it with a different name on the switch.

Related command: **tftp put**.

Example

Download the file LANSwitch.app from the TFTP server at `1.1.3.214` and save it as `vxWorks.app` on the local switch.

```
<SW4500>tftp 1.1.3.214 get LANSwitch.app vxWorks.app
```

tftp put

Syntax

tftp *tftp-server* put *source-file* [*dest-file*]

View

User view

Parameter

tftp-server: IP address or hostname of the TFTP server. The name of the TFTP server should be a string ranging from 1 to 20 characters.

source-file: Specify the filename of the source file which is saved on the switch.

dest-file: Specify the filename of the destination file which will be saved on the TFTP server.

Description

Use the **tftp put** command to upload a file from the switch to the specified directory on the TFTP server and save it with a new name.

Related commands: **tftp get**.

Example

```
<SW5500>tftp 1.1.3.214 put sw5500cfg.txt temp.txt
```

MAC Address Table Management Commands

This section describes the commands you can use to manage the MAC Address Table on your Switch 4500.

display mac-address

Syntax

display mac-address [***mac-addr*** **[vlan** ***vlan-id*** **]** | **[static** | **dynamic** | **blackhole] [interface** { ***interface-name*** | ***interface-type interface-num*** } **] [vlan** ***vlan-id*** **] [count]]**

View

All views

Parameter

mac-addr: Specify the MAC address.

vlan-id: Specify the VLAN ID.

static: Static table entry, lost after resetting switch.

dynamic: Dynamic table entry, which will be aged.

blackhole: Blackhole table entry, the packet with this destination MAC address will be discarded.

interface-type: Specify the interface type.

interface-num: Specify the interface number.

interface-name: Specify the interface name.

For details about the ***interface-type***, ***interface-num*** and ***interface-name*** parameters, refer to the Port Configuration in this manual.

count: the display information will only contain the number of MAC addresses in the MAC address table if the user enters this parameter when using this command.

Description

Use the **display mac-address** command to display MAC address table information.

When managing the Layer-2 addresses of the switch, the administrator can perform this command to view such information as the Layer-2 address table, address status (static or dynamic), Ethernet port of the MAC address, VLAN of the address, and system address aging time.

For the related commands, see **mac-address**, **mac-address timer**.

Example

Show the information of the entry with MAC address at 00e0-fc01-0101

```
<SW4500>sys
System View: return to User View with Ctrl+Z.
[SW4500]display mac-address 00e0-fc01-0101
MAC ADDR        VLAN ID    STATE      PORT INDEX      AGING TIME(s)
00e0-fc01-0101  1          Learned    Ethernet1/0/1   300
```

display mac-address aging-time

Syntax

display mac-address aging-time

View

All views

Parameter

None

Description

Use the **display mac-address aging-time** command to display the aging time of the dynamic entry in the MAC address table.

For the related commands, see **mac-address**, **mac-address timer**, **display mac-address**.

Examples

Display the aging time of the dynamic entry in the MAC address table.

```
<SW4500>sys
System View: return to User View with Ctrl+Z.
[SW4500]display mac-address aging-time
mac-address aging-time: 300s
```

The above information indicates that the aging time of the dynamic entry in the MAC address is 300s.

```
<SW4500>sys
System View: return to User View with Ctrl+Z.
[SW4500] display mac-address aging-time
mac-address aging-time: no-aging
```

The above information indicates that the dynamic entry in the MAC address table is no-aging.

mac-address

Syntax

mac-address { static | dynamic | blackhole } ***mac-address*** **interface {** ***interface-name*** **|** ***interface-type interface-num*** **} vlan** ***vlan-id***

undo mac-address [{ static | dynamic | blackhole } *mac-address* interface { *interface-name* | *interface-type interface-num*] vlan *vlan-id*]

View

System view

Parameter

static: Static table entry, lost after resetting switch.

dynamic: Dynamic table entry, which will be aged.

blackhole: Blackhole table entry, the packet with this destination MAC address will be discarded.

mac-addr: Specify the MAC address.

interface-type: Specify the interface type.

interface-num: Specify the interface number.

interface-name: Specify the interface name.

vlan-id: Specify the VLAN ID.

Description

Use the **mac-address** command to add/modify the MAC address table entry. Use the **undo mac-address** command to delete MAC address table entry

If the input address has been existing in the address table, the original entry will be modified. That is, replace the interface pointed by this address with the new interface and the entry attribute with the new attribute (dynamic entry and static entry).

All the (MAC unicast) addresses on a certain interface can be deleted. User can choose to delete any of the following addresses: address learned by system automatically, dynamic address configured by user, static address configured by user.

For the related commands, see **display mac-address**.

Example

Configure the port number corresponding to the MAC address 00e0-fc01-0101 as Ethernet1/0/1 in the address table, and sets this entry as static entry.

```
<SW4500>sys
System View: return to User View with Ctrl+Z.
[SW4500]mac-address static 00e0-fc01-0101 interface Ethernet 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

Parameter

count: Enter a value in the range 0 to 32768 to specify how many MAC addresses a port can learn. 0 means that the port is not allowed to learn MAC addresses.

Description

Use the **mac-address max-mac-count** command to configure the maximum number of MAC addresses that can be learned by a specified Ethernet port. The port stops learning MAC addresses when the specified limit is reached.

Use the **undo mac-address-table max-mac-count** command to cancel the maximum limit on the number of MAC addresses learned by an Ethernet port. This is the default. If you set no maximum limit, the MAC address table controls the number of MAC addresses a port can learn.

Related commands: **mac-address**, **mac-address timer**

Examples

To configure the port "Ethernet 1/0/3" to learn at most 600 MAC addresses, enter the following:

```
<SW4500>sys
System View: return to User View with Ctrl+Z.
[SW4500]interface Ethernet 1/0/3
[SW4500-Ethernet1/0/3]mac-address max-mac-count 600
```

To cancel the maximum limit on the number of MAC addresses learned by the port "Ethernet1/0/3", enter the following:

```
<SW4500>sys
System View: return to User View with Ctrl+Z.
[SW4500]interface Ethernet 1/0/3
[SW4500-Ethernet1/0/3]undo mac-address max-mac-count
```

mac-address timer

Syntax

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

undo mac-address timer aging

View

System view

Parameter

aging *age*: Specifies the aging time (measured in seconds) of the Layer-2 dynamic address table entry, ranging from 10 to 1000000; by default, the aging time is 300 seconds.

no-aging: No aging time.

Description

Use the **mac-address timer** command to configure the aging time of the Layer-2 dynamic address table entry. Use the **undo mac-address timer** command to restore the default value.

Setting the aging time on the switch to be too long or too short will cause the switch to broadcast data packets without MAC addresses, this will affect the operational performance of the switch.

If the aging time is set too long, the switch will store out-of-date MAC address tables. This will consume MAC address table resources and the switch will not be able to update MAC address table according to the network change.

If aging time is set too short, the switch may delete valid MAC address table entries.

Example

Configure the entry aging time of Layer-2 dynamic address table to be 500 seconds.

```
<SW4500>sys
System View: return to User View with Ctrl+Z.
[SW4500]mac-address timer aging 500
```

Device Management Commands

This section describes the device management commands available on your Switch 4500.

boot boot-loader

Syntax

boot boot-loader ***file-path***

View

User view

Parameter

file-path: Path and name of APP file.

Description

Use the **boot boot-loader** command to specify the app file used for booting next time.

You can not specify the app file stored in another Unit as the boot application of a Unit.

Example

Specify the APP application used for booting next time.

```
<SW4500>boot boot-loader unit1>flash:/PLATV100R002B09D002.APP The
specified file will be booted next time!
<SW4500>
```

boot bootrom

Syntax

boot bootrom ***file-path***

View

User view

Parameter

file-path: File path and file name of Bootrom.

Description

Use the **boot bootrom** command to upgrade bootrom.

Example

Upgrade bootrom of the switch.

```
<SW4500>boot bootrom PLATV100R002B09D002.btm
```

display boot-loader

Syntax

display boot-loader [unit *unit-id*]

View

All views

Parameter

unit *unit-id*: Specify the Unit ID of the switch.

Description

Use the **display boot-loader** command to display APP file used for this boot and the next boot.

Example

```
<SW4500>display boot-loader
The app to boot at the next time is: flash:/platform.app
The app to boot of board 0 at this time is:
flash:/PLATV100R002B09D002.APP
```

display cpu

Syntax

display cpu [unit *unit-id*]

View

All views.

Parameter

unit *unit-id*: Specify the Unit ID of the switch.

Description

Use the **display cpu** command to display CPU occupancy.

Example

To display CPU occupancy, enter the following:

```
<SW4500>display cpu
```

The information displays in the following format:

```
Unit 1
Board 0 CPU busy status:
   11% in last 5 seconds
   12% in last 1 minute
   14% in last 5 minutes
```

Table 32 Display information

Field	Description
Board 0 CPU busy status	The busy status of the Switch
11% in last 5 seconds	The CPU occupancy rate is 11% at last 5 seconds
12% in last 1 minute	The CPU occupancy rate is 12% at last 1 minute
14% in last 5 minutes	The CPU occupancy rate is 14% at last 5 minutes

display device

Syntax

display device [unit *unit-id*]

View

All views

Parameter

unit *unit-id*: Specify the Unit ID of the switch.

Description

Use the **display device** command to display the module type and working status information of a card, including physical card number, physical daughter card number, number of ports, hardware version number, FPGA version number, version number of BOOTROM software, application version number, address learning mode, interface card type and interface card type description, etc.

Example

Show device information.

```
<SW4500>display device

Unit 1
SlotNo SubSNo PortNum PCBVer FPGAVer CPLDVer BootRomVer AddrLM Type State
0      0      24      REV.A  NULL    000     200        IVLMAIN Norma
```

display fan

Syntax

display fan [unit *unit-id*]

View

All views

Parameter

unit *unit-id:* Specify the Unit ID of the switch

Description

Use the **display fan** command to display the working state of the built-in fans.

Example

Display the working state of the fans.

```
<SW4500>display fan
Unit 1
Fan 1 State: Normal
```

The above information indicates that the fan works normally.

display memory

Syntax

display memory [unit *unit-id*]

View

All views

Parameter

unit *unit-id*: Specify the Unit ID of the switch

Description

Use the **display memory** command to display the current system memory status.

Example

To display the current memory status, enter the following:

```
<SW4500>display memory
```

The information displays in the following format:

```
Unit 1
System Available Memory(bytes): 31608192
System Used Memory(bytes): 14723652
Used Rate: 46%
```

Table 33 Display information

Field	Description
System Available Memory (bytes)	The Total Memory of switch, unit in byte
System Used Memory (bytes)	The Total used Memory of switch, unit in byte
Used Rate	The memory used rate

display power

Syntax

display power [unit *unit-id*][*power-ID*]

View

All views

Parameter

unit *unit-id*: Specify the Unit ID of the switch

power-ID: Power ID.

Description

Use the **display power** command to display the working state of the built-in power supply.

Example

Show power state.

```
<SW4500>display power 1
Unit1
power 1 State: Normal
```

display schedule reboot

Syntax

display schedule reboot

View

Any view

Parameter

None

Description

Use the **display schedule reboot** command to check the configuration of related parameters of the switch schedule reboot terminal service.

Related command: **reboot, schedule reboot at, schedule reboot delay, undo schedule reboot.**

Example

Display the configuration of the schedule reboot terminal service parameters of the current switch.

```
<SW4500>display schedule reboot

System will reboot at 03:41 2000/04/02 (in 1 hours and 27 minutes).
```

reboot

Syntax

reboot [unit *unit-id*]

View

User view

Parameter

unit *unit-id*: Specify the Unit ID of the switch

Description

Use the **reboot** command to reset the Switch when failure occurs.

Example

Reboots the Switch.

```
<SW4500>reboot
This will reboot device. Continue? [Y/N]
```

schedule reboot at

Syntax

schedule reboot at hh:mm [yyyy/mm/dd]

undo schedule reboot

View

User view

Parameter

hh:mm: Reboot time of the switch, in the format of "hour: minute" The hh ranges from 0 to 23, and the mm ranges from 0 to 59.

yyyy/mm/dd: Reboot date of the switch, in the format of "year/month/day. The yyyy ranges from 2000 to 2099, the mm ranges from 1 to 12, and the value of dd is related to the specific month.

Description

Use the **schedule reboot at** command to enable the timing reboot function of the switch and set the specific reboot time and date.

Use the **undo schedule reboot** command to disable the timing reboot function.

By default, the timing reboot switch function is disabled.

If the **schedule reboot at** command sets specified date parameters, which represents a data in the future, the switch will be restarted in specified time, with error not more than 1 minute.

If no specified date parameters are configured, two cases are involved: If the configured time is after the current time, the switch will be restarted at the time point of that day; if the configured time is before the current time, the switch will be restarted at the time point of the next day.

It should be noted that the configured date should not exceed the current date more than 30 days. In addition, after the command is configured, the system will prompt you to input confirmation information. Only after the "Y" or the "y" is entered can the configuration be valid. If there is related configuration before, it will be covered directly.

After the **schedule reboot at** command is configured and the system time is adjusted by the **clock** command, the former configured **schedule reboot at** parameter will go invalid.

For the related command, see **reboot, schedule reboot delay, display schedule reboot.**

Example

Set the switch to be restarted at 22:00 that night (the current time is 15:50).

```
<SW4500>schedule reboot at 22:00
Reboot system at 22:00:00 2000/04/02 (in 19 hours and 47 minutes)
confirm? [Y/N]:y
%Apr  2 02:12:20:72 2000 3Com CMD/5/REBOOT:- 1 -
aux0: schedule reboot parameters at 02:12:20 2000/04/02. And system
will reboot at 22:00 2000/04/02.
<SW4500>
```

schedule reboot delay

Syntax

schedule reboot delay { *hhh:mm* | *mmm* }

undo schedule reboot

View

User view

Parameter

hhh:mm: Waiting time for rebooting a switch, in the format of "hour: minute" The hhh ranges from 0 to 720, and the mm ranges from 0 to 59.

mmm: Waiting delay for rebooting a switch, in the format of "absolute minutes" . Ranging from 0 to 43200,

Description

Use the **schedule reboot delay** command to enable the timing reboot switch function and set the waiting time. Use the **undo schedule reboot** command to disable the timing reboot function.

By default, the timing reboot switch function is disabled.

Two formats can be used to set the waiting delay of timing reboot switch, namely the format of "hour: minute" and the format of "absolute minutes". But the total minutes should be no more than 30×24×60 minutes, or 30 days.

After this command is configured, the system will prompt you to input confirmation information. Only after the "Y" or the "y" is entered can the configuration be valid. If there is related configuration before, it will be covered directly.

After the **schedule reboot at** command is configured, and the system time is adjusted by the **clock** command, the original **schedule reboot at** parameter will become invalid.

For the related command, see **reboot, schedule reboot at, undo schedule reboot, display schedule reboot**

Example

Configure the switch to be restarted after 88 minutes (the current time is 21:32).

```
<SW4500>schedule reboot delay 88
Reboot system at 03:41 2000/04/02 (in 1 hours and 28 minutes)
```

```
Confirm? [Y/N]:y
%Apr  2 02:13:10:09 2000 3Com CMD/5/REBOOT:- 1 -
aux0: schedule reboot parameters at 02:13:10 2000/04/02. And system
will reboot at 03:41 2000/04/02.
<SW5500>
```

Basic System Configuration and Management Commands

This section describes the basic system configuration and system management commands available on your Switch 4500.

clock datetime

Syntax

clock datetime ***time date***

View

User view

Parameters

time **:** Enter the current time in ***HH:MM:SS*** format . *HH* can be in the range 0 to 23. *MM* and *SS* can be in the range 0 to 59.

date : Enter the current year in ***MM/DD/YYYY*** or ***YYYY/MM/DD*** format . ***YYYY*** can be in the range 2000 to 2099. ***MM*** can be in the range 1 to 12. ***DD*** can be in the range 1 to 31.

Description

Use the **clock datetime** command to set the current system time and date. The default is 23:55:52, 2000/4/1.

Related command: **display clock**

Example

To set the system time and date to 09:30:00, 2004/1/1, enter the following:

```
<SW4500>clock datetime 09:30:00 2004/01/01
```

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: Enter the name of the summer time zone, up to 32 characters in length.

one-off: Specifies that the summer time is set for the selected year.

repeating: Specifies that the summer time is set for every year, starting from the selected year.

start_time: Enter the start time of summer time, in the format HH:MM:SS.

start_date: Enter the start date of summer time, in the format YYYY/MM/DD.

end_time: Enter the end time of summer time, in the format HH:MM:SS.

end_date: Enter the end date of summer time, in the format YYYY/MM/DD.

offset_time: Enter the offset time, that is the amount of time added, in the format HH:MM:SS.

Description

Use the **clock summer-time** command to set the name, start date and time, and end date and time of summer time.

Use the **undo clock summer-time** command to cancel the currently configured summer time.

Use the **display clock** command to check the summer time settings.

Related command: **clock timezone**

Example

To set the summer time for zone 2 to start at 06:00:00 on 08/06/2002, and end at 06:00:00 on 01/09/2002, with a time added of one hour, enter the following:

```
<SW4500>clock summer-time z2 one-off 06:00:00 2002/06/08 06:00:00
2002/09/01 01:00:00
```

To set the summer time for zone 2 to start at 06:00:00 on 08/06, and end at 06:00:00 on 01/09 in each year starting in 2002, with a time added of one hour, enter the following:

```
<SW4500>clock summer-time z2 repeating 06:00:00 2002/06/08 06:00:00
2002/09/01 01:00:00
```

clock timezone

Syntax

clock timezone ***zone_name*** **{ add | minus }** ***HH:MM:SS***

undo clock timezone

View

User view

Parameter

zone_name: Enter the name of the time zone, up to 32 characters in length.

add: Specifies that time is ahead of UTC.

minus: Specifies that time is behind UTC.

HH:MM:SS: Enter the time difference between the time zone and UTC.

Description

Use the **clock timezone** command to set local time zone information.

Use the **undo clock timezone** command to return to the default, which is Universal Time Coordinated (UTC).

Use the **display clock** command to check the summer time settings.

Related command: **clock summer-time**

Example

To set the local time zone as zone 5, and configure the local time to be 5 hours ahead of UTC, enter the following:

```
<SW4500>clock timezone z5 add 05:00:00
```

sysname

Syntax

sysname sysname

undo sysname

View

System view

Parameter

sysname: Specify the hostname with a character string with the length ranging from1 to 30 characters.

Description

Use the **sysname** command to set the system name of the Switch.

Using **undo sysname** command, you can restore the default value of the system name.

By default, the system name of the Switch is SW4500.

Changing the system name of the Switch will affect the prompt of the command line interface. For example, the system name of the Switch is SW4500, and the prompt in user view is <SW4500>.

Example

Set the hostname of the Switch to be LANSwitch.

```
<5500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]sysname LANSwitch
[LANSwitch]
```

System Status and System Information Display Commands

This sections describes the system status and system information display commands on your Switch 4500.

display clock

Syntax

display clock

View

All views

Parameter

None

Description

Use the **display clock** command to obtain information about system data and time from the terminal display..

For the related commands, see **clock**.

Example

View the current system date and clock.

```
<SW4500>display clock
15:50:45 UTC Mon 01/01/2001
```

display config-agent

Syntax

display config-agent unit-id *unit-id*

View

Any view

Parameter

***unit-id*:** Unit ID of current switch, in the range of 1 to 8.

Description

Use the **display config-agent unit-id** command to view statistics of the configuration agent.

Configuration agent is one of the XRN features. You can log into one switch of the fabric to configure and manage the fabric by the configuration agent. The functions of the configuration agent include;

- Distributing configuration commands to the right destination switches or processing modules based on the resolution result of the commands input.
- Sending output information of the commands from the switch you have logged into to your terminal.
- Supporting simultaneous configuration of multiple users.

You cannot configure the configuration agent, but can view the statistics of the configuration agent.

Example

To display statistics of the configuration agent on switch 1, enter the following:

```
<SW4500>display config-agent unit-id 1
Config-agent statistic information on Unit1
Message type            Successful                    Failed on
Config message recv:          0                           0
```

```
Config message send:          0                              0
Notification message recv:    0                              0
Notification message send:    0                              0
Information message recv:     0                              0
Information message send:     0                              0
```

display debugging

Syntax

display debugging [interface { *interface-name* | *interface-type interface-num* }] [*module-name*]

View

All views

Parameter

interface-name: Specify the Ethernet port name.

interface-type: Specify the Ethernet port type.

interface-num: Specify the Ethernet port number.

module-name: Specify the module name.

Description

Use the **display debugging** command to display the enabled debugging process.

Show all the enabled debugging when there is no parameter.

For the related commands, see **debugging**.

Example

Show all the enabled debugging.

```
<SW4500>display debugging
IP packet debugging switch is on.
```

display version

Syntax

display version

View

All views

Parameter

None

Description

Use the **display version** command to view the software version, issue date and the basic hardware configuration information.

Example

Display the information about the system version.

```
<SW4500>display version
```

System Debug Commands

This section describes the system debugging options, and the system diagnostics information that can be displayed on your Switch 4500.

debugging

Syntax

debugging *module-name* [*debugging-option*]

undo debugging { all | *module-name* [*debugging-option*] }

View

User view

Parameter

all: Disable all the debugging.

timeout *interval*: The interval during which the debugging command is valid. The ***interval*** value can range from 1 to 1440 minutes.

module-name: Specify the module name.

debugging-option: Debugging option.

Description

Use the **debugging** command to enable the system debugging. Use the **undo debugging** command to disable the system debugging.

By default, all the debugging processes are disabled.

The Switch provides various kinds of debugging functions for technical support personnel and experienced maintenance staff to troubleshoot the network.

Enabling the debugging will generate a large amount of debugging information and decrease the system efficiency. If the **debugging all** command is used, it will adversely affect the operational performance of the network. Use the **undo debugging all** command to disable all debugging.

By default, if multiple devices form a fabric, the debugging information of the master is broadcasted within the fabric and the debugging information of the slave is only displayed on the slave device. You can view the debugging information including that of the master and the device in which the login port resides.

You can enable the logging, debugging and trap information switches within the fabric by executing the i**nfo-center switch-on all** command. Synchronization is a process that each switch sends its own information to the other switches in the fabric, and meantime receives information from others to update local information, ensuring the consistency of logging, debugging and trap information in a fabric.

After the synchronization of the whole fabric, a great deal of terminal display is generated. You are recommended not to enable the information synchronization switch of the whole fabric. If you enabled the information synchronization switch,

after the synchronization information statistics and detection, you must execute the **undo info-center switch-on** *command to disable the switch in time.*

For the related commands, see **display debugging**.

Example

Enable IP Packet debugging.

```
<SW4500>debugging ip packet
IP packet debugging switch is on.
```

display diagnostic-information

Syntax

display diagnostic-information

View

All views

Parameter

None

Description

Use the **display diagnostic-information** command to view the configuration information on all currently running modules. This information helps you to monitor and troubleshoot your Switch 4500.

Example

To display system information on all currently running modules, enter the following:

```
<SW4500>display diagnostic-information
```

Network Connection Test Commands

This section describes the network connection test commands available on your Switch 4500.

end-station polling ip-address

Syntax

end-station polling ip-address ***ip-address***

undo end-station polling ip-address ***ip-address***

View

System view

Parameter

ip-address: Specify the IP address.

Description

Use the **end-station polling ip-address** command to configure the IP address requiring periodic testing.

Use the **undo end-station polling ip-address** command to delete the IP address requiring periodic testing.

The switch can ping an IP address every one minute to test if it is reachable. Three PING packets can be sent at most for every IP address in every testing with a time interval of five seconds. If the switch cannot ping successfully the IP address after the three PING packets, it assumes that the IP address is unreachable.

You can configure up to 50 IP addresses by using the command repeatedly.

Related command: **ping**, **tracert**.

Example

Configure 202.38.160.244 requiring periodical testing.

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]end-station polling ip-address 202.38.160.244
```

ping

Syntax

ping [-a *ip-address*] [-c *count*] [-d] [-h *tll*][-i {*interface-type interface-num* | *interface-name* }][ip] [-n] [- p *pattern*] [-q] [-r] [-s *packetsize*] [-t *timeout*] [-tos *tos*] [-v] *string*

View

User view

Parameter

-a *ip-address:* Specify the source IP address to transmit ICMP ECHO-REQUEST.

-c: ***count*** specify how many times the ICMP ECHO-REQUEST packet will be transmitted, ranging from 1 to 4294967295.

-d: Configure the socket to be in DEBUGGING mode.

-h *ttl*: Configure TTL value for echo requests to be sent, range from 1 to 255

-i: Configure to choose packet sent on the interface.

interface-type: Specify the interface type.

interface-num: Specify the interface number.

interface-name: Specify the interface name.

ip: Choose IP ICMP packet.

-n: Configure to take the host parameter as IP address without domain name resolution.

-p: ***pattern*** is the hexadecimal padding of ICMP ECHO-REQUEST, e.g. -p ff pads the packet completely with ff.

-q: Configure not to display any other detailed information except statistics.

-r: Record route.

-s *packetsize:* Specify the length of ECHO-REQUEST (excluding IP and ICMP packet header) in bytes.

-t *timeout:* Maximum waiting time after sending the ECHO-REQUEST (measured in ms).

-tos *tos:* Specify TOS value for echo requests to be sent, range from 0 to 255.

-v: Show other received ICMP packets (non ECHO-RESPONSE).

string: Destination host domain name or IP address.

Description

Use the **ping** command to check the IP network connection and the reachability of the host.

By default, when the parameters are not specified:

- the ECHO-REQUEST message will be sent for 5 times,
- socket is not in DEBUGGING mode,
- the TTL value for echo requests is 255,.
- host will be treated as IP address first. If it is not an IP address, perform domain name resolution,
- the default padding operation starts from 0x01 and ends on 0x09 (progressively), then performs again,
- show all the information including statistics,
- routes are not recorded,
- send ECHO-REQUEST according to route selection,
- default length of ECHO-REQUEST is 56 bytes.,
- default timeout of ECHO-RESPONSE is 2000ms,
- do not display other ICMP packets (non ECHO-RESPONSE),
- the TOS value of echo requests is 0.

The **ping** command sends ICMP ECHO-REQUEST message to the destination. If the network to the destination works well, then the destination host will send ICMP ECHO-REPLY to the source host after receiving ICMP ECHO-REQUEST.

Perform the **ping** command to troubleshoot the network connection and line quality. The output information includes:

- Responses to each of the ECHO-REQUEST messages. If the response message is not received until timeout, output "Request time out". Or display response message bytes, packet sequence number, TTL and response time.

- The final statistics, including number of sent packets, number of response packets received, percentage of non-response packets and minimal/maximum/average value of response time.

If the network transmission rate is too low to increase the response message timeout.

For the related commands, see **tracert**.

Example

Check whether the host 202.38.160.244 is reachable.

```
<SW4500>ping 202.38.160.244
ping 202.38.160.244 : 56 data bytes
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 packets transmitted
5 packets received
0% packet loss
round-trip min/avg/max = 1/2/3 ms
```

remote-ping

Purpose

Use the **remote-ping** command to specify remote-ping test class.

Syntax

```
remote-ping [ count | destination-ip | display | frequency |
msdp-tracert | mtracert | ping | quit ]
```

Parameters

count	Specifies remote-ping probe number in one test.
destination-ip	Specifies remote-ping class destination ip address.
display	Displays current system information.
frequency	Specifies remote-ping interval time between two remote-ping tests.
msdp-tracert	Specifies MSDP trace route to source RP.
mtracert	Traces route to multicast source.
ping	Ping function.
quit	Exits from current command view.

Example

```
[5500-EI]remote-ping
```

View

This command can be used in the following views:

- System view

Description

Remote-ping is a network diagnostic tool used to test the performance of protocols (only ICMP by far) operating on network. It is an enhanced alternative to the ping command.

Remote-ping test group is a set of remote-ping test parameters. A test group contains several test parameters and is uniquely identified by an administrator name plus a test tag.

You can perform an remote-ping test after creating a test group and configuring the test parameters.

Different from the ping command, remote-ping does not display the round trip time (RTT) and timeout status of each packet on the console terminal in real time. You need to execute the display remote-ping command to view the statistic results of your remote-ping test operation. remote-ping allows administrators to set the parameters of remote-ping test groups and start remote-ping test operations.

Related Commands

display remote-ping

ping

tracert

display remote-ping

Purpose

Use the **display remote-ping** command to display the test results.

Syntax

display remote-ping { results | history } [***administrator-name test-tag***]

Parameters

results	Displays the latest test results.
history	Displays the test history.
administrator-name	Name of the administrator who created the test.
test-tag	Test tag.

Example

Display the latest test results of the test group administrator icmp.

```
<S5500> display remote-ping results administrator icmp
Remote-ping entry(admin administrator, tag icmp) test result:
```

```
  Destination ip address:10.10.10.10
  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 complete 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 34 Description on the fields of the display remote-ping results command

Field	Description
Destination ip address	Destination IP address
Send operation times	Packet sending times
Receive response times	Successful packet sending times
Min/Max/Average Round Trip Time	Min/max/average round trip time (RTT)
Square-Sum of Round Trip Time	Quadratic sum of RTTs
Last complete test time	Time of the last successful send operation in the test
SD Maximal delay	Max delay from the source to the destination
DS Maximal delay	Max delay from the destination to the source
Packet lost in test	Rate of the lost packets in the test
Disconnect operation number	Number of the disconnect operations forcibly performed by the opposite party
Operation timeout number	Number of the send operations getting no response within the timeout time in the test
System busy operation number	Number of the failed send operations due to system busy in the test
Connection fail number	Number of the failed attempts to establish a connection with the opposite party.
Operation sequence errors	Number of the out-of-sequence packets received
Drop operation number	Number of the failed system resource assignment operations
Other operation errors	Number of other errors

Display the test history of the test group administrator icmp.<S5500> 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 35 Description on the fields of the display remote-ping history command

Field	Description
Response	Round trip time in ms or timeout time. It is 0 if the test fails.
Status	Result value of the send operation, including: 1: responseReceived 2: unknown 3: internalError 4: requestTimedOut 5: unknownDestinationAddress 6: noRouteToTarget 7: interfaceInactiveToTarget 8: arpFailure 9: maxConcurrentLimitReached 10: unableToResolveDnsName 11: invalidHostAddress
LastRC	Last response code received (this code is based on the specific implementation). When the ICMP Echo function is enabled, if an ICMP response containing ICMP_ECHOREPLY(0) is received, it indicates the detection succeeds.
Time	Test time

View

This command can be used in the following views:

- Any view

Description

If a test group is specified by using the administrator-name and test-tag arguments, the system displays the test results of the specified test group. Otherwise the system displays the test results of all the test groups.

Related Commands

`remote-ping`

`test-enable`

remote-ping-agent enable

Purpose

Use the **`remote-ping-agent enable`** command to enable remote-ping client.

Use the **`undo remote-ping-agent enable`** command to disable remote-ping client.

Syntax

remote-ping-agent enable

undo remote-ping-agent enable

Parameters

None

Example

Enable remote-ping client.

```
[S5500] remote-ping-agent enable
```

View

This command can be used in the following views:

- System view

Description

You can perform a test only after the remote-ping client function is enabled.

tracert

Syntax

tracert [[-a *source-ip*] -f *first-TTL*] [-m *max-TTL*] [-p *port*] [-q *nqueries*] [-w *timeout*] *string*

View

All views

Parameter

-a *source-IP*: Configure the source IP address used by tracert command.

-f: Configure to verify the -f switch, ***first-TTL*** specifies an initial TTL, ranging from 0 to the maximum TTL.

-m: Configure to verify the -m switch, ***max-TTL*** specifies a maximum TTL larger than the initial TTL.

-p: Configure to verify the -p switch, ***port*** is an integer host port number. Generally, user need not modify this option.

-q: Configure to verify the -q switch, ***nqueries*** is an integer specifying the number of query packets sent, larger than 0.

-w: Configure to verify the -w switch, ***timeout*** is an integer specifying IP packet timeout in seconds, larger than 0.

string: IP address of the destination host or the hostname of the remote system.

Description

Use the **tracert** command to check the reachability of network connection and troubleshoot the network. User can test gateways passed by the packets transmitted from the host to the destination.

By default, when the parameters are not specified,

first-TTL is 1,

max-TTL is 30,

port is 33434,

nqueries is 3 and

timeout is 5s.

The **tracert** command sends a packet with TTL 1, and the first hop will send an ICMP error message back to indicate this packet cannot be transmitted (because of TTL timeout). Then this packet will be sent again with TTL 2, and the second hop will indicate a TTL timeout error. Perform this operation repeatedly till reaching the destination. These processes are operated to record the source address of each ICMP TTL timeout so as to provide a path to the destination for an IP packet.

After the **ping** command finds some error on the network, perform **tracert** to locate the error.

The output of the **tracert** command includes IP address of all the gateways to the destination. If a certain gateway times out, output "***".

Example

Test the gateways passed by the packets to the destination host at 18.26.0.115.

```
<SW4500>tracert 18.26.0.115
tracert to allspice.lcs.mit.edu (18.26.0.115), 30 hops max
1 helios.ee.lbl.gov (128.3.112.1) 0 ms 0 ms 0 ms
2 lilac-dmc.Berkeley.EDU (128.32.216.1) 19 ms 19 ms 19 ms
3 lilac-dmc.Berkeley.EDU (128.32.216.1) 39 ms 19 ms 19 ms
4 ccngw-ner-cc.Berkeley.EDU (128.32.136.23) 19 ms 39 ms 39 ms
5 ccn-nerif22.Berkeley.EDU (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 ALLSPICE.LCS.MIT.EDU (18.26.0.115) 339 ms 279 ms 279 ms
```

Log Commands

This section displays the logging options available on your Switch 4500.

display channel

Syntax

display channel [***channel-number*** | ***channel-name*** **]**

View

All views

Parameter

channel-number: Channel number, ranging from 0 to 9, that is, the system has ten channels.

channel-name: Specify the channel name, the name can be **console, monitor, loghost, trapbuffer, logbuffer, snmpagent, channel6, channel7, channel8, channel9.** Where console is channel 0, monitor is channel 1, loghost is channel 2, trapbuffer is channel 3, logbuffer is channel 4 and snmpagent is channel 5.

Description

Use the **display channel** command to display the details about the information channel.

Without a parameter, the **display channel** command shows the configurations of all the channels.

Example

Show details about the information channel 0.

```
<SW4500>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

View

All views

Parameter

None

Description

Use the **display info-center** command to display the configuration of system log and the information recorded in the memory buffer.

If the information in the current log/trap buffer is less than the specified *sizeval*, display the actual log/trap information.

For the related commands, see **info-center enable**, **info-center loghost**, **info-center logbuffer**, **info-center console channel**, **info-center monitor channel**.

Example

Show the system log information.

```
<SW4500>display info-center
Information Center: enabled
Log host:
         173.168.1.10, 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:256
         current messages:6, channel number:4, channel name:logbuffer
         dropped messages:0, overwrote messages:0
Trap buffer:
         enabled, max buffer size:1024, current buffer size:256
         current messages:0, channel number:3, channel
name:trapbuffer
         dropped messages:0, overwrote messages:0
Information timestamp setting:
         log - date, trap - date, debug - boot
XRN SWITCH OF this Device: LOG = disable; TRAP = disable; DEBUG =
enable
```

info-center channel name

Syntax

info-center channel *channel-number* name *channel-name*
undo info-center channel *channel-number*

View

System view

Parameter

channel-number: Channel number, ranging from 0 to 9, that is, system has ten channels.

channel-name: Specify the channel name with a character string not exceeding 30 characters, excluding "-", "/" or "\".

Description

Use the **info-center channel name** command to rename a channel specified by the ***channel-number*** as ***channel-name.*** . Using the u**ndo info-center channel command**, you can restore the channel name.

Note that the channel name cannot be duplicated.

Example

Rename channel 0 as execconsole.

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]info-center channel 0 name execconsole
[SW4500]
```

info-center console channel

Syntax

info-center console channel { *channel-number* | *channel-name* }

undo info-center console channel

View

System view

Parameter

channel-number: Channel number, ranging from 0 to 9, that is, system has ten channels.

channel-name: : Specify the channel name. The name can be **channel6, channel7, channel8, channel9, console, logbuffer, loghost, monitor, snmpagent, trapbuffer.**

Description

Use the **info-center console channel** command to configure the channel through which the log information is output to the console.

By default, the Switch 4500 does not output log information to the console.

This command takes effect only after system logging is started.

For the related commands, see **info-center enable**, **display info-center**.

Example

Configure to output log information to the console through channel 0.

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]info-center console channel 0
[SW4500]
```

info-center enable

Syntax

info-center enable

undo info-center enable

View

System view

Parameter

None

Description

Use the **info-center enable** command to enable the system log function. Use the **undo info-center enable** command to disable system log function.

By default, system log function is enabled.

Only after the system log function is enabled can the system output the log information to the info-center loghost and console, etc.

For the related commands, see **info-center loghost**, **info-center logbuffer**, **info-center console channel**, **info-center monitor channel**, **display info-center**.

Example

Enable the system log function.

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]info-center enable
% Information center is enabled
[SW4500]
```

info-center logbuffer

Syntax

info-center logbuffer [channel { ***channel-number*** | ***channel-name*** **}** | **size** ***buffersize*** **]**
undo info-center logbuffer [channel | **size]**

View

System view

Parameter

channel: Configure the channel to output information to buffer.

channel-number: Channel number, ranging from 0 to 9, that is, system has ten channels.

channel-name: Specify the channel name. The name can be **channel6, channel7, channel8, channel9, console, logbuffer, loghost, monitor, snmpagent, trapbuffer.**

size: Configure the size of buffer.

buffersize: Size of buffer (number of messages which can be kept); The default size of the buffer is 512.

Description

Use the **info-center logbuffer** command to configure to output information to the memory buffer. Use the **undo info-center logbuffer** command to cancel the information output to buffer

This command takes effect only after the system logging is enabled.

For the related commands, see **info-center enable**, **display info-center**.

Example

Send log information to buffer and sets the size of buffer as 50.

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]info-center logbuffer 50
[SW4500]
```

info-center loghost

Syntax

info-center loghost ***host-ip-addr*** **[channel** { ***channel-number*** | ***channel-name*** } | **facility** ***local-number*** | **language** { **chinese** | **english** } **]**

undo info-center loghost ***host-ip-addr***

View

System view

Parameter

host-ip-addr: IP address of info-center loghost.

channel: Configure information channel of the info-center loghost.

channel-number: Channel number, ranging from 0 to 9, that is, system has ten channels.

channel-name: Specify the channel name. The name can be **channel6, channel7, channel8, channel9, console, logbuffer, loghost, monitor, snmpagent, trapbuffer.**

facility: Configure the recording tool of info-center loghost.

local-number: Record tool of info-center loghost, ranging from local0 to local7.

language: Set the logging language.

chinese, english: Language used in log file.

Description

Use the **info-center loghost** command to set the IP address of the info-center loghost to send information to it. Use the **undo info-center loghost** command to cancel output to info-center loghost.

By default, switches do not output information to info-center loghost.

This command takes effect only after the system logging is enabled.

For the related commands, see **info-center enable**, **display info-center**.

Example

Configure to send log information to the UNIX workstation at 202.38.160.1.

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]info-center loghost 202.38.160.1
[SW4500]
```

info-center loghost source

syntax

info-center loghost source ***interface-name***

undo info-center source

View

System view

Parameter

source interface-name*:** Sets the source address of packets sent to the loghost as the address of the interface specified by ***interface-name. Normally, the interface is a VLAN interface.

Description

Use the **info-center loghost source** command to set the source address of packets sent to the loghost as the address of the interface specified by the ***interface-name*** parameter.

Use the **undo info-center loghost source** command to cancel the setting of the source address of the packets sent to the loghost.

This command takes effect only after the system logging is enabled.

Related commands: **info-center enable**, **display info-center**.

Example

Set the source address of the packets sent to the loghost as the address of the VLAN interface 1.

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]info-center loghost source vlan-interface 1
[SW4500]
```

info-center monitor channel

Syntax

info-center monitor channel { ***channel-number*** | ***channel-name*** }

undo info-center monitor channel

View

System view

Parameter

channel-number: Channel number, ranging from 0 to 9, that is, the system has ten channels.

channel-name: Specify the channel name. The name can be **channel6, channel7, channel8, channel9, console, logbuffer, loghost, monitor, snmpagent, trapbuffer.**

Description

Use the **info-center monitor channel** command to set the channel to output the log information to the user terminal.

Use **undo info-center monitor channel** command to restore the channel to output the log information to the user terminal to the default value.

By default, switches do not output log information to user terminal.

This command takes effect only after system logging is started.

For the related commands, see **info-center enable**, **display info-center**.

Example

Configure channel 0 to output log information to user terminal.

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]info-center monitor channel 0
[SW4500]
```

info-center snmp channel

Syntax

info-center snmp channel { *channel-number* | *channel-name* }

undo info-center snmp channel

View

System view

Parameter

channel-number: Channel number, ranging from 0 to 9, that is, the system has ten channels. By default, channel 5 is used.

channel-name: Specify the channel name. The name can be **channel6, channel7, channel8, channel9, console, logbuffer, loghost, monitor, snmpagent, trapbuffer.**

Description

Use the **info-center snmp channel** command to specify new channel for transmitting the SNMP information.

Use **undo info-center snmp channel** command to restore the channel for transmitting the SNMP information to default value.

Related commands: **display snmp.**

Example

Configure channel 6 as the SNMP information channel.

```
<SW4500>system-view
```

```
System View: return to User View with Ctrl+Z.
[SW4500]info-center snmp channel 6
[SW4500]
```

info-center source

Syntax

info-center source { *modu-name* | default } channel { *channel-number* | *channel-name* } [debug { level *severity* | state *state* }* | log { level *severity* | state *state* }* | trap { level *severity* | state *state* }] *

undo info-center source { *modu-name* | default } channel { *channel-number* | *channel-name* }

View

System view

Parameter

***modu-name*:** Module name. See Table 36.

default: All the modules.

log: Log information.

trap: Trap information.

debugging: Debugging information.

level: Level.

***severity*:** Information level, do not output information below this level. By default, the log information level is warnings, the trap information level is debugging, the debugging information level is debugging.

Information at different levels is as follows:

emergencies: Level 1 information, which cannot be used by the system.

alerts: Level 2 information, to be reacted immediately.

critical: Level 3 information, critical information.

errors: Level 4 information, error information.

warnings: level 5 information, warning information.

notifications: Level 6 information, showed normally and important.

informational: Level 7 information, notice to be recorded.

debugging: Level 8 information, generated during the debugging progress.

If you only specify the level for one or two of the three types of information, the level(s) of the unspecified type(s) return to the default. For example, if you only define the level of the log information, then the levels of the trap and debugging information return to the defaults.

***channel-number*:** Channel number to be set.

channel-name: Channel name to be set. The name can be **channel6, channel7, channel8, channel9, console, logbuffer, loghost, monitor, snmpagent, trapbuffer.**

state: Set the state of the information.

state: Specify the state as **on** or **off**.

Table 36 Module names in logging information

Module name	Description
8021X	802.1X module
ACL	Access control list module
AM	Access management module
ARP	Address resolution protocol module
CFAX	Configuration proxy module
CFG	Configuration management platform module
CFM	Configuration file management module
CMD	Command line module
COMMONSY	Common system MIB module
DEV	Device management module
DHCC	DHCP Client module
DHCP	Dynamic host configuration protocol module
DRV	Driver module
DRV_MNT	Driver maintenance module
ESP	End-station polling module
ETH	Ethernet module
FIB	Forwarding module
FTM	Fabric topology management module
FTMCMD	Fabric topology management command line module
FTPS	FTP server module
HA	High availability module
HTTPD	HTTP server module
IFNET	Interface management module
IGSP	IGMP snooping module
IP	IP module
IPC	Inter-process communication module
IPMC	IP multicast module
L2INF	Interface management module
LACL	LANswitch ACL module
LQOS	LANswitch QoS module
LS	Local server module
MPM	Multicast port management module
NTP	Network time protocol module
PPRDT	Protocol packet redirection module
PTVL	Driver port, VLAN (Port & VLAN) module

Table 36 Module names in logging information

Module name	Description
QACL	QoS/ACL module
QOSF	Qos profile module
RDS	Radius module
RM	Routing management
RMON	Remote monitor module
RSA	Revest, shamir and adleman encryption system
RTPRO	Routing protocol
SHELL	User interface
SNMP	Simple network management protocol
SOCKET	Socket
SSH	Secure shell module
STP	Spanning tree protocol module
SYSMIB	System MIB module
TELNET	Telnet module
UDPH	UDP helper module
VFS	Virtual file system module
VTY	Virtual type terminal module
WCN	Web management module
XM	XModem module

Description

Use the **`info-center source`** command to add/delete a record to the information channel. Use the **`undo info-center source`** command to delete the contents of the information channel.

For example, for the filter of IP module log output, you can configure to output the logs at a level higher than warnings to the log host and output those higher than informational to the log buffer. You can also configure to output the trap information on the IP module to a specified trap host, etc.

The channels for filtering in all the directions are specified by this configuration command. All the information will be sent to the corresponding directions through the specified channels. You can configure the channels in the output direction, channel filter information, filtering and redirecting of all kinds of information.

At present, the system distributes an information channel in each output direction by default, shown as follows:

Table 37 Information Channel in Each Output Direction by Default

Output direction	Information channel name
Console	console
Monitor	monitor
Info-center loghost	loghost
Log buffer	logbuffer

Table 37 Information Channel in Each Output Direction by Default

Trap buffer	trapbuffer
snmp	snmpagent

In addition, each information channel has a default record with the module name "all" and module number as 0xffff0000. However, for different information channel, the default log, trap and debugging settings in the records may be different with one another. Use default configuration record if a module does not have any specific configuration record in the channel.

Example

Configure to enable the log information of STP module in SNMP channel and allows the output of the information with a level no higher than emergencies.

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]info-center source stp channel snmpagent log level
emergencies
[SW4500]
```

info-center switch-on

Syntax

info-center switch-on { *unit-id* | master | all } [debugging | logging | trapping]*

undo info-center switch-on { *unit-id* | *master* | all } [debugging | logging | trapping]*

View

System view

Parameter

unit-id: Unit ID of switch.

master: Master switch of Fabric.

all: All switches of Fabric.

debugging: Debugging information.

logging: Log information.

trapping: Trap information.

Description

Use the **info-center switch-on** command to turn on the information synchronization switch of the specified switch.

Use the **undo info-center switch-on** command to turn off the information synchronization switch of the specified switch.

By default, the debugging information synchronization switch on master unit is enabled, log information and trap information switches on master unit are disabled, all information synchronization switches on slave unit are disabled.

After the forming of a Fabric by switches which support the XRN, the log, debugging and trap information among the switches is synchronous. The synchronization process is as follows: each switch sends its own information to other switches in the Fabric and meantime receives the information from others, and then the switch updates the local information to ensure the information coincidence within the Fabric.

The switch provides command line to turn on/off the synchronization switch in every switch. If the synchronization switch of a switch is turned off, it does not send information to other switches but still receives information from others.

Example

To turn on the trapping information synchronization switch of the unit 2, enter the following:

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]info-center switch-on 2 trapping
[SW4500]
```

info-center timestamp

Syntax

info-center timestamp { log | trap | debugging } { boot | date | none }

undo info-center timestamp { log | trap | debugging }

View

System view

Parameter

log: Log information.

trap: Trap information.

debugging: Debugging information.

boot: Time elapsing after system starts. Format: xxxxxx.yyyyyy, xxxxxx is the high 32 bits of the elapsed time (in milliseconds) after system starts, and yyyyyy is the low 32 bits.

date: Current system date and time. It shows as `yyyy/mm/dd-hh:mm:ss` in Chinese environment and `mm/dd/yyyy-hh:mm:ss` in Western language environment.

None: No timestamp format.

Description

Use the **info-center timestamp** command to configure the timestamp output format in debugging/trap information. Use the **undo info-center timestamp** command to disable the output of timestamp field.

By default, datetime stamp is used.

Example

Configure the debugging information timestamp format as boot.

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]info-center timestamp debugging boot
[SW4500]
```

info-center trapbuffer

Syntax

info-center trapbuffer [size *buffersize*] [channel { ***channel-number*** | ***channel-name*** **}]**

undo info-center trapbuffer [channel | **size]**

View

System view

Parameter

size: Configure the size of the trap buffer.

buffersize: Size of trap buffer (numbers of messages).

channel: Configure the channel to output information to trap buffer.

channel-number: Channel number, ranging from 0 to 9, that is, the system has ten channels.

channel-name: Specify the channel name.

Description

Use the **info-center trapbuffer** command to output information to the trap buffer. Use the **undo info-center trapbuffer** command to cancel output information to trap buffer.

By default, output information is transmitted to trap buffer and size of trap buffer is 256.

This command takes effect only after the system logging is enabled.

Related commands: **info-center enable, display info-center**.

Example

Send information to the trap buffer and sets the size of buffer as 30.

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]info-center trapbuffer size 30
[SW4500]
```

reset logbuffer

Syntax

reset logbuffer

View

User view

Parameter

None

Description

Use the **reset logbuffer** command to clear information in log buffer.

Example

Clear information in log buffer.

```
<SW4500>reset logbuffer
```

reset trapbuffer

Syntax

reset trapbuffer

View

User view

Parameter

None

Description

Use the **reset trapbuffer** command to clear information in trap buffer.

Example

Clear information in trap buffer.

```
<SW4500>reset trapbuffer
```

terminal debugging

Syntax

terminal debugging

undo terminal debugging

View

User view

Parameter

None

Description

Use the **terminal debugging** command to configure to display the debugging information on the terminal. Use the **undo terminal debugging** command to configure not to display the debugging information on the terminal.

By default, the displaying function is disabled.

Related commands: **debugging.**

Example

Enable the terminal display debugging.

```
<SW4500>terminal debugging
% Current terminal debugging is on
<SW4500>
```

terminal logging

Syntax

terminal logging

undo terminal logging

View

User view

Parameter

None

Description

Use the **terminal logging** command to start logging the information displayed on the terminal. Use the **undo terminal logging** command to disable terminal log information display.

By default, this function is enabled.

Example

Disable the terminal log display.

```
<SW4500>undo terminal logging
% Current terminal logging is off
<SW4500>
```

terminal monitor

Syntax

terminal monitor

undo terminal monitor

View

User view

Parameter

None

Description

Use the **terminal monitor** command to enable the log debugging/log/trap on the terminal monitor. Use the **undo terminal monitor** command to disable these functions.

By default, enable these functions for the console user and disable them for the terminal user.

This command only takes effect on the current terminal where the commands are input. The debugging/log/trap information can be output to the current terminal, beginning in user view. When the terminal monitor is shut down, no debugging/log/trap information will be displayed in local terminal, which is equals to having performed the **undo terminal debugging**, **undo terminal logging**, undo terminal trapping commands. When the terminal monitor is enabled to use **terminal debugging / undo terminal debugging**, **terminal logging / terminal logging and terminal trapping / undo terminal trapping** respectively to enable or disable the corresponding functions.

Example

Disable the terminal monitor.

```
<SW4500>undo terminal monitor
% Current terminal monitor is off
<SW4500>
```

terminal trapping

Syntax

terminal trapping

undo terminal trapping

View

User view

Parameter

None

Description

Use the **terminal trapping** command to enable terminal trap information display. Use the **undo terminal trapping** command to disable this function.

By default, this function is enabled.

Example

Enable trap information display.

```
<SW4500>terminal trapping
% Current terminal trapping is on
<SW4500>
```

SNMP Configuration Commands

This section displays the Simple Network Management Protocol (SNMP) commands available on your Switch 4500.

display snmp-agent

Syntax

display snmp-agent { local-engineid | remote-engineid }

View

All views

Parameter

local-engineid: local engine ID.

remote-engineid: remote engine ID.

Description

Use the **display snmp-agent engineid** command to view the engine ID of current device.

SNMP engine is the core of SNMP entity. It performs the function of sending, receiving and authenticating SNMP message, extracting PDU, packet encapsulation and the communication with SNMP application, etc.

Example

Display the engine ID of current device.

```
<SW4500>display snmp-agent engineid
Local SNMP engineID: 000000090200000000C025808
```

display snmp-agent community

Syntax

display snmp-agent community [read | write]

View

All views

Parameter

read: display read-only community information.

write: display read-write community information.

Description

Use the **display snmp-agent community** command to display the currently configured community names.

Example

Display the currently configured community names.

```
<SW4500>display snmp-agent community
community name:public
group name:public
storage-type: nonVolatile

community name:tom
group name:3Com
storage-type: nonVolatile
```

display snmp-agent group

Syntax

display snmp-agent group [*group-name*]

View

All views

Parameter

groupname: Group name, ranging from 1 to 32 bytes.

Description

Use the **display snmp-agent group** command to display group name, safe mode, state of various views and storage modes.

Example

Display SNMP group name and safe mode.

```
<SW4500>display snmp-agent group
groupname: public
Security model: v2c noAuthnoPriv
readview:v1default
writeview: no writeview specified
notifyview: *tv.FFFFFFFF
storage-type: volatile
```

The following table describes the output fields.

Table 38 Output description of the display snmp-agent group command

Field	Description
groupname	SNMP Group name of the user
Security model	The security model adopted by SNMP
readview	Read-only MIB view name corresponding to that group
writeview	Writable MIB view corresponding to that group
notifyview	The name of the notify MIB view corresponding to that group
storage-type	Storage type

display snmp-agent mib-view

Syntax

display snmp-agent mib-view [exclude | **include** | **viewname** ***mib-view*** **]**

View

All views

Parameter

exclude: Display the SNMP mib view excluded.

include: Display the SNMP mib view included.

viewname: Display the SNMP mib view according to the mib view name.

mib-view: Specify the mib view name.

Description

The **display snmp-agent mib-view** command is used to view the MIB view configuration information of the Switch.

Example

Display the information about the currently configured MIB view.

```
<SW4500>display snmp-agent mib-view
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
```

If the SNMP Agent is disabled, "Snmp Agent disabled" will be displayed after you execute the above ***display*** *commands.*

display snmp-agent statistics

Syntax

display snmp-agent statistics

View

All views

Parameter

None

Description

Use the **display snmp-agent statistics** command to view the current state of SNMP communication.

This command provides a counter for SNMP operations.

Example

Display the current state of SNMP communication.

```
<SW4500>display snmp-agent statistics
0 Messages delivered to the SNMP entity
0 Messages which were for an unsupported version
0 Messages which used an unknown community name
0 Messages which represented an illegal operation for the community
supplied
0 ASN.1 or BER errors in the process of decoding
0 MIB objects retrieved successfully
0 MIB objects altered successfully
0 Get-request PDUs accepted and processed
0 Get-next PDUs accepted and processed
0 Set-request PDUs accepted and processed
```

```
3 Messages passed from the SNMP entity
0 SNMP PDUs which had a tooBig error (Maximum packet size 1500)
0 SNMP PDUs which had a noSuchName error
0 SNMP PDUs which had a badValue error
0 SNMP PDUs which had a general error
0 Response PDUs accepted and processed
3 Trap PDUs accepted and processed
```

The following table describes the output fields.

Table 39 Output description of the display snmp-agent statistics command

Field	Description
0 Messages delivered to the SNMP entity	Total number of the input SNMP packets
0 Messages which were for an unsupported version	Number of packets with version information error
0 Messages which used an unknown community name	Number of packets with community name error
0 Messages which represented an illegal operation for the community supplied	Number of packets with authority error corresponding to the community name
0 ASN.1 or BER errors in the process of decoding	Number of SNMP packets with encoding error
0 MIB objects retrieved successfully	Number of variables requested by NMS
0 MIB objects altered successfully	The number of variables set by NMS
0 Get-request PDUs accepted and processed	Number of the received packets requested by get
0 Get-next PDUs accepted and processed	Number of the received packets requested by get-next
0 Set-request PDUs accepted and processed	Number of the received packets requested by set
3 Messages passed from the SNMP entity	Total number of the output SNMP packets
0 SNMP PDUs which had a tooBig error (Maximum packet size 1500)	Number SNMP packet with too_big error
0 SNMP PDUs which had a noSuchName error	Number of the packets requesting nonexistent MIB objects
0 SNMP PDUs which had a badValue error	Number of SNMP packets with Bad_values error
0 SNMP PDUs which had a general error	Number of SNMP packets with General_errors
0 Response PDUs accepted and processed	Number of the response packets sent
3 Trap PDUs accepted and processed	Number of the sent Trap packets

display snmp-agent sys-info

Syntax

display snmp-agent sys-info [contact | location | version]*

View

All views

Parameter

None

Description

Use the **display snmp-agent sys-info** command to view the system information of SNMP configuration. The information includes the character string sysContact (system contact), the character string describing the system location, the version information about the running SNMP in the system.

Example

Display the character string sysContact (system contact).

```
<SW4500>display snmp-agent sys-info contact
The contact person for this managed node:
Mr.Smith -Tel:3306
```

Display the system location.

```
<SW4500>display snmp-agent sys-info location
The physical location of this node:
Boston USA
```

Display the version information of running SNMP

```
<SW4500>display snmp-agent sys-info version
SNMP version running in the system:
SNMPv3
```

display snmp-agent usm-user

Syntax

display snmp-agent usm-user [engineid *engineid* | group *groupname* | username *username*]

View

All views

Parameter

engineid: display user information with specified engine ID.

username: display user information with specified user name.

groupname: display user information of specified group.

Description

Use the **display snmp-agent usm-user** command to view information of all the SNMP usernames in the group username list.

Example

Display the information of all the current users.

```
<SW4500>display snmp-agent usm-user
User name: hello
   Group name: hellogroup
       Engine ID: 800007DB00E0FC0039006877
       Storage-type: nonVolatile
       UserStatus: active
       Acl:2000
```

display snmp-proxy unit

Syntax

display snmp-proxy unit *unit-id*

View

Any view

Parameter

unit-id:Unit ID of the switch.

Description

Using **display snmp-proxy unit** command, you can view statistics information of SNMP proxy.

Example

View statistics information of SNMP proxy on unit 1.

```
<SW4500> display snmp-proxy unit 1
Number of GetReq msgs received :0
Number of GetReq msgs sent :0

Number of GetNextReq msgs Received :0
Number of GetNextReq msgs sent :0

Number of GetResp msgs received :0
Number of GetResp msgs sent :0

Number of GetNextResp msgs received :0
Number of GetNextResp msgs sent :0

Number of SnmpMibSync msgs received :0
Number of SnmpMibSync msgs sent :0

Number of SnmpMibGetCntrReq msgs received :0
Number of SnmpMibGetCntrReq msgs sent :0

Number of SnmpMibGetCntrResp msgs received :0
Number of SnmpMibGetCntrResp msgs sent :0
```

enable snmp trap

Syntax

enable snmp trap updown
undo enable snmp trap updown

View

Ethernet port view

Parameter

None.

Description

Use the **enable snmp trap updown** command to enable the current port to transmit the LINK UP and LINK DOWN trap information.

Use the **undo enable snmp trap updown** command to disable the current port to transmit the LINK UP and LINK DOWN trap information.

Example

Enable the current port Ethernet1/0/1 to transmit the LINK UP and LINK DOWN trap information.

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]interface Ethernet 1/0/1
[SW4500-Ethernet1/0/1]enable snmp trap updown
[SW4500-Ethernet1/0/1]
```

snmp-agent community

Syntax

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

undo snmp-agent community ***community-name***

View

System view

Parameter

read: Indicate that MIB object can only be read.

write: Indicate that MIB object can be read and written.

community-name: Community name character string.

view-name: MIB view name.

acl ***acl-list*****:** set access control list for specified community.

Description

Use the **snmp-agent community** command to set the community access name and enable access to SNMP. Use the **undo snmp-agent community** command to cancel the settings of community access name.

Example

Configure community name as **comaccess** and with read-only access permission.

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]snmp-agent community read comaccess
[SW4500]
```

Configure community name as **mgr** and read-write access permission.

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]snmp-agent community write mgr
[SW4500]
```

Delete the community name **comaccess**.

```
[SW4500]undo snmp-agent community comaccess
```

snmp-agent group

Syntax

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

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

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

View

System view

Parameter

group-name: Enter a group name, up to 32 characters in length.

authentication: Specifies that the packet is authenticated without encryption.

privacy: Specifies that the packet is authenticated and encrypted.

read-view: Configures read-only view settings.

read-view: Enter a read-only view name, up to 32 characters in length.

write-view: Configures read and write view settings.

write-view: Enter a read and write view name, up to 32 characters in length.

notify-view: Configures notify view settings.

notify-view: Enter a notify view name, up to 32 characters in length.

acl *acl-list*: Enter the access control list for this group name.

v3: Configures SNMP version 3.

Description

Use the **snmp-agent group** command to configure a new SNMP group, that is, map an SNMP user to SNMP view.

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

3Com recommends that you do not use the **notify-view** parameter when configuring an SNMP group, for the following reasons:

- The **snmp-agent target-host** command automatically generates a *notify-view* for a user, and adds it to the corresponding group.
- Any change of the SNMP group *notify-view* will affect all the users related to this group.

Example

To create an SNMP group named 3Com, enter the following:

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]snmp-agent group v3 3Com
[SW4500]
```

snmp-agent local-engineid

Syntax

snmp-agent local-engineid ***engineid***

undo snmp-agent local-engineid

View

System view

Parameter

local-engineid: Specify an engineID for the local SNMPv3 entity

engineid: Specify the engine ID with a character string, only composed of hexadecimal numbers between 5 and 32 inclusive. The default value is "Enterprise Number + device information".

Description

Use the **snmp-agent local-engineid** command to configure a name for a local or remote SNMP engine on the Switch. Use the **undo snmp-agent local-engineid** command to restore the default setting of engine ID.

Device information is determined according to different products. It can be IP address, MAC address or user defined text. However, you must use numbers in hexadecimal form.

Example

Configure the ID of a local or remote device as 1234512345.

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
<SW4500>snmp-agent local-engineid 1234512345
<SW4500>
```

snmp-agent mib-view

Syntax

snmp-agent mib-view { included | **excluded }** ***view-name oid-tree***

undo snmp-agent mib-view ***view-name***

View

System view

Parameter

included: Include this MIB subtree.

excluded: Exclude this MIB subtree.

view-name: Specify the view name, with a character string, ranging from 1 to 32 characters.

oid-tree: MIB object subtree. It can be a character string of the variable OID, or a variable name, ranging from 1 to 255 characters.

Description

Use the **snmp-agent mib-view** command to create or update the view information. Use the **undo snmp-agent mib-view** command to delete the view information

By default, the view name is v1default. OID is 1.3.6.1.

Both the character string of OID and the node name can be input as parameter.

Example

Create a view that consists of all the objects of MIB-II.

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]snmp-agent mib-view included mib2 1.3.6.1.3
[SW4500]
```

snmp-agent packet max-size

Syntax

snmp-agent packet max-size ***byte-count***

undo snmp-agent packet max-size

View

System view

Parameter

byte-count: Specify the size of SNMP packet (measured in bytes), ranging from 484 to 17940; the default size is 1500 bytes.

Description

Use the **snmp-agent packet max-size** command to configure the size of SNMP packet that the Agent can send/receive. Use the **undo snmp-agent packet max-size** command to restore the default size of SNMP packet.

The sizes of the SNMP packets received/sent by the Agent are different in different network environments.

Example

Set the size of SNMP packet to 1042 bytes.

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]snmp-agent packet max-size 1042
[SW4500]
```

snmp-agent sys-info

Syntax

snmp-agent sys-info { contact *sysContact* | location *sysLocation* | version { { v1 | v2c | v3 } * | all } }

undo snmp-agent sys-info [{ contact | location }* | version { { v1 | v2c | v3 }* | all }]

View

System view

Parameter

sysContact: Specify a character string describing the system maintenance contact (in bytes), with a length ranging from 1 to 255. The default contact information is "3Com Marlborough USA".

sysLocation: Specify a character string to describe the system location. By default, the character string is "Marlborough USA".

version: version of running SNMP.

v1: SNMP v1.

v2c: SNMP v2C.

v3: SNMP v3.

all: all SNMP version (includes SNMP v1, SNMP v2C, SNMP v3).

Description

Use the **snmp-agent sys-info** command to set system information such as geographical location of the device, contact information for system maintenance and version information of running SNMP. Use the **undo snmp-agent sys-info location** command to restore the default value.

Example

Set system location as Building 3/Room 214.

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]snmp-agent sys-info location Building 3/Room 214
[SW4500]
```

snmp-agent target-host

Syntax

snmp-agent target-host trap address udp-domain *host-addr* [udp-port *udp-port-number*] params securityname *community-string* [v1 | v2c | v3 [authentication | privacy]]

undo snmp-agent target-host *host-addr* securityname *community-string*

View

System view

Parameter

trap: Specifies the host to receive traps or notifications

address: Specifies the transport address to be used in the generation of SNMP messages.

udp-domain: Specifies the transport domain over UDP for the target address.

host-addr: Enter the IP address of the destination host.

udp-port *udp-port-number:* Enter the UDP port number of the host to receive the SNMP notification.

params: Specifies the SNMP target information to be used in the generation of SNMP messages.

community-string: Enter the community name, up to 32 characters in length.

v1: Specifies SNMP version v1.

v2c: Specifies SNMP version v2C.

v3: Specifies SNMP version v3.

authentication: Specifies that the packet is authenticated without encryption.

privacy: Specifies that the packet is authenticated and encrypted.

community-string: Specifies the community name. The character string ranges from1 to 32 bytes.

Description

Use the **snmp-agent target-host** command to select and configure the host that you want to receive SNMP notification.

Use the **undo snmp-agent target-host** command to cancel the host currently configured to receive SNMP notification.

You must enter the **snmp-agent trap enable** command before you enter the **snmp-agent target-host** command. The **snmp-agent trap enable** command enables the device to transmit Trap packets. To send Trap messages, at least one **snmp-agent target-host** command should be configured.

Example

To enable Trap messages to be sent to **2.2.2.2** with a community name of **comaccess**, enter the following:

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]snmp-agent trap enable
```

```
[SW4500]snmp-agent target-host trap address udp-domain 2.2.2.2
params securityname comaccess
[SW4500]
```

To enable Trap messages to be sent to **2.2.2.2** with a community name of **public**, enter the following:

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]snmp-agent trap enable
[SW4500]snmp-agent target-host trap address udp-domain 2.2.2.2
params securityname public
[SW4500]
```

snmp-agent trap enable

Syntax

snmp-agent trap enable [configuration | **flash** | **ospf [** ***process-id*** **]**
[***ospf-trap-list*** **]** | **standard [authentication** | **coldstart** | **linkdown**
| **linkup** | **warmstart]*** | **system]**

undo snmp-agent trap enable [bgp [backwardtransition] [
established] | **configuration** | **flash** | **ospf [** ***process-id*** **] [**
ospf-trap-list **]** | **standard [authentication** | **coldstart** | **linkdown** |
linkup | **warmstart]*** | **system]**

View

System view

Parameter

configuration: Configure to send SNMP configuration Trap packets.

flash: Configure to send SNMP flash Trap packets.

ospf [***process-id*** **] [** ***ospf-trap-list*** **]**: Configure to send the OSPF trap packets. ***process-id*** is the ID of the OSPF process, ranging from 1 to 65535. ***ospf-trap-list*** is the list of OSPF trap information.

standard [authentication | **coldstart** | **linkdown** | **linkup** | **warmstart**
]*: Configure to send standard Trap messages.

authentication: Configure to send SNMP authentication Trap messages when authentication fails.

coldstart: Configure to send SNMP cold start Trap messages when switch is rebooted.

linkdown: Configure to send SNMP link down Trap messages when switch port turns down.

linkup: Configure to send SNMP link up Trap messages when switch port turns up.

warmstart: Configure to send SNMP warm start Trap messages when snmp is re-enabled.

system: Configure to send SysMib trap messages.

Description

Use the **snmp-agent trap enable** command to enable the device to send Trap message. Use the **undo snmp-agent trap enable** command to disable Trap message sending.

By default, Trap message sending is disabled.

The **snmp-agent trap enable** command and the **snmp-agent target-host** command should be used at the same time. The **snmp-agent target-host** command specifies which hosts can receive Trap message. To send Trap messages, at least one **snmp-agent target-host** command should be configured.

Example

Enable to send the trap packet of SNMP authentication failure to **10.1.1.1**. The community name is **3Com**.

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]snmp-agent trap enable standard authentication
[SW4500]snmp-agent target-host trap address udp-domain 10.1.1.1
param securityname 3Com
[SW4500]
```

snmp-agent trap life

Syntax

snmp-agent trap life ***seconds***

undo snmp-agent trap life

View

System view

Parameter

seconds: Specify the timeouts, ranging from 1 to 2592000 seconds. By default, the timeout interval is 120 seconds.

Description

Use the **snmp-agent trap life** command to set the timeout of Trap packets. Use the **undo snmp-agent trap life** command to restore the default value.

The set timeout of Trap packet is represented by ***seconds***. If time exceeds ***seconds***, this Trap packet will be discarded.

For the related commands, see **snmp-agent trap enable**, **snmp-agent target-host**.

Example

Configure the timeout interval of Trap packet as 60 seconds.

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]snmp-agent trap life 60
[SW4500]
```

snmp-agent trap queue-size

Syntax

snmp-agent trap queue-size ***length***

undo snmp-agent trap queue-size

View

System view

Parameter

length: Length of queue, ranging from 1 to 1000; the default length is 100.

Description

Use the **snmp-agent trap queue-size** command to configure the information queue length of Trap packet sent to destination host. Use the **undo snmp-agent trap queue-size** command to restore the default value.

For the related commands, see **snmp-agent trap enable**, **snmp-agent target-host**, **snmp-agent trap life**.

Example

Configure the queue length to 200.

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]snmp-agent trap queue-size 200
[SW4500]
```

snmp-agent trap source

Syntax

snmp-agent trap source vlan-interface ***vlan-id***

undo snmp-agent trap source

View

System view

Parameter

vlan-id: Specify the VLAN interface ID, ranging from 1 to 4094.

Description

Use the **snmp-agent trap source** command to specify the source address for sending Traps. Use the **undo snmp-agent trap source** command to cancel the source address for sending Traps.

Example

Configure the IP address of the VLAN interface 1 as the source address for transmitting the Trap packets.

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]snmp-agent trap source vlan-interface 1
[SW4500]
```

snmp-agent usm-user

Syntax

snmp-agent usm-user { v1 | v2c } *username groupname* [acl *acl-list*]

undo snmp-agent usm-user { v1 | v2c } *username groupname*

snmp-agent usm-user v3 *username groupname* [authentication-mode { md5 | sha } *authpassstring* [privacy-mode { des56 *privpassstring* }]] [acl *acl-list*]

undo snmp-agent usm-user v3 *username groupname* { local | engineid *engine-id* }

View

System view

Parameter

username: Enter the user name, up to 32 characters in length.

groupname: Enter the group name corresponding to that user, up to 32 characters in length.

v1: Specifies the use of v1 safe mode.

v2c: Specifies the use of v2c safe mode.

v3: Specifies the use of v3 safe mode.

authentication-mode: Specifies the use of authentication.

md5: Specifies that the MD5 algorithm is used in authentication. MD5 authentication uses a128-bit password. The computation speed of MD5 is faster than that of SHA

sha: Specifies that the SHA algorithm is used in authentication. SHA authentication uses a 160-bit password. The computation speed of SHA is slower than that of MD5, but SHA offers higher security.

authpassstring: Enter the authentication password, up to 64 characters in length.

privacy-mode: Specifies the use of authentication and encryption.

des 56: Specifies that the DES encryption algorithm is used. Must be entered if you enter the **privacy-mode** parameter.

privpassstring: Enter the encryption password with a character string, ranging from 1 to 64 bytes.

acl *acl-list*: Enter the access control list for this user, based on USM name.

Description

Use the **snmp-agent usm-user** command to add a new community name or, if you use the V3 parameter, a new user to an SNMP group.

Use the **undo snmp-agent usm-user** command to delete a user from an SNMP group.

SNMP engineID (for authentication) is required when configuring remote users. This command will not be effective if engineID is not configured.

For v1 and v2C, this command will add a new community name. For v3, it will add a new user for an SNMP group. See Related Commands below.

Related commands: **display snmp-agent**, **snmp-agent local engineid**

Example

To add a user named "JohnQ" to the SNMP group "3Com", then configure the use of MD5, and set the authentication password to "pass", enter the following:

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]snmp-agent usm-user v3 JohnQ 3Com authentication-mode md5
pass
[SW4500]
```

undo snmp-agent

Syntax

undo snmp-agent

View

System view

Parameter

None

Description

Use the **undo snmp-agent** command to disable all versions of SNMP running on the server.

Any **snmp-agent** command will enable SNMP Agent.

Example

Disable the running SNMP agents of all SNMP versions.

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]undo snmp-agent
[SW4500]
```

RMON Configuration Commands

This section describes the Remote Monitoring (RMON) configuration commands available on your Switch 4500.

display rmon alarm

Syntax

display rmon alarm [*alarm-table-entry*]

View

All views

Parameter

alarm-table-entry: Alarm table entry index.

Description

Use the **display rmon alarm** command to view RMON alarm information.

For the related commands, see **rmon alarm.**

Example

Display the RMON alarm information.

```
<SW4500>display rmon alarm
Alarm table 1 owned by 3COM is VALID.
  Samples absolute value : 1.3.6.1.2.1.16.1.1.1.4.1
<etherStatsOctets.1>
  Sampling interval          : 10(sec)
  Rising threshold           : 1000(linked with event 1)
  Falling threshold          : 100(linked with event 1)
  When startup enables       : risingOrFallingAlarm
  Latest value               : 0
```

Table 40 Output description of the display rmon alarm command

Field	Description
Alarm table 1	Index 1 in the alarm table
3Com	Owner
VALID	The entry corresponding to the index is valid
Samples absolute value	Sampling the absolute value of the node 1.3.6.1.2.1.16.1.1.1.4.1
Sampling interval	The interval of sampling the value
Rising threshold1	Rising threshold. When sampling value rises from normal value to this threshold, rising threshold alarm will be triggered.
Falling threshold	Falling threshold. When sampling value decreases from normal value to this threshold, falling threshold alarm will be triggered.
startup	The first trigger
risingOrFallingAlarm	The type of the first alarm: Specifies to alarm when exceeding the rising threshold or the falling threshold

display rmon event

Syntax

display rmon event [*event-table-entry*]

View

All views

Parameter

event-table-entry: Entry index of event table.

Description

Use the **display rmon event** command to view RMON events.

The display includes event index in event table, owner of the event, description to the event, action caused by event (log or alarm information), and occurrence time of the latest event (counted on system initiate/boot time in centiseconds).

Related command: **rmon event.**

Example

Show the RMON event.

```
<SW4500>display rmon event
Event table 1 is VALID, and owned by 3COM.
   Description: null.
   Will cause log-trap when triggered, last triggered at 0days
00h:02m:27s.
```

Table 41 Output description of the display rmon event command

Field	Description
Event table 1	Index 1 in event table
VALID	The entry corresponding to the index is valid
3COM	Owner
Description	Event description
Will cause log-trap when triggered, last triggered at 0days 00h:02m:27s	When the event is triggered, it will cause the log-trap. And the last triggered time is 00h:02m:27s

display rmon eventlog

Syntax

display rmon eventlog [***event-number*** **]**

View

All views

Parameter

event-number: Entry index of event table.

Description

Use the **display rmon eventlog** command to display RMON event log.

The display includes description about event index in event table, description to the event, and occurrence time of the latest event (counted on system initiate/boot time in centiseconds).

Example

Show the RMON event log.

```
<SW4500>display rmon eventlog 1
Event table 1 owned by 3Com 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 42 Output description of the display rmon eventlog command

Field	Description
Event table 1	Index 1 in event table
3Com	Owner
VALID	The entry corresponding to the index is valid
Description	Event description
less than (or =) 100 with alarm value 0	The alarm sample value is less than or equal to 100
Alarm sample type is absolute	The type of alarm sampling is absolute
Generates eventLog 1.2 at 0days 00h:02m:27s	The eventlog corresponding to the index 1.2 is generated at 0days 00h:02m:27s.

display rmon history

Syntax

display rmon history [*port-num*]

View

All views

Parameter

port-num: Ethernet port name.

Description

Use the **display rmon history** command to view the latest RMON history sampling information (including utility, error number and total packet number).

For the related commands, see **rmon history**.

Example

Show the RMON history information.

```
<SW4500>display rmon history ethernet 2/0/1
History control entry 1 owned by 3Com is VALID,
   Samples interface     : Ethernet1/0/1<ifEntry.642>
   Sampling interval     : 10(sec) with 10 buckets max
   Latest sampled values :
   Dropevents        :0         , octets               :0
   packets           :0         , broadcast packets    :0
   multicast packets :0         , CRC alignment errors :0
   undersize packets :0         , oversize packets     :0
   fragments         :0         , jabbers              :0
   collisions        :0         , utilization          :0
```

Table 43 Output description of the display rmon history command

Field	Description
History control table	Index number in history control table
3COM	Owner
VALID	The entry corresponding to the index is valid
Samples interface	The sampled interface
Sampling interval	Sampling interval
buckets	Records in history control table
dropevents	Dropping packet events
octets	Sent/received octets in sampling time
packets	Packets sent/received in sampling time
broadcastpackets	Number of broadcast packets
multicastpackets	Number of multicast packets
CRC alignment errors	Number of CRC error packets
undersized	Number of undersized packets
oversized packets	Number of oversized packets
fragments	Number of undersized and CRC error packets
jabbers	Number of oversized and CRC error packets
collisions	Number of collision packets
utilization	Utilization

display rmon prialarm

Syntax

display rmon prialarm [*prialarm-table-entry*]

View

All views

Parameter

prialarm-table-entry: entry of extended alarm table.

Description

Use the **display rmon prialarm** command to display information about extended alarm table.

Related command: **rmon prialarm**.

Example

Display alarm information about extended RMON.

```
<SW4500>display rmon prialarm
Prialarm table 1 owned by 3Com is VALID.
  Samples    absolute value : .1.3.6.1.2.1.16.1.1.1.4.1
  Sampling interval         : 10(sec)
  Rising threshold          : 1000(linked with event 1)
  Falling threshold         : 100(linked with event 1)
  When startup enables      : risingOrFallingAlarm
  This entry will exist     : forever.
  Latest value              : 0
```

Table 44 Output description of the display rmon prialarm command

Field	Description
Prialarm table 1	Index of extended alarm entry.
owned by 3COM	Creator of the extended alarm entry.
VALID	The entry corresponding to the index is valid
Samples absolute value	Sampling the absolute value of the node 1.3.6.1.2.1.16.1.1.1.4.1
Rising threshold	Rising threshold. When sampling value rises from normal value to this threshold, rising threshold alarm will be triggered.
Falling threshold	Falling threshold. When sampling value decreases from normal value to this threshold, falling threshold alarm will be triggered.
linked with event 1	Corresponding event index of ring and falling threshold alarm.
When startup enables: risingOrFallingAlarm	Kind of first alarm. It may trigger rising threshold alarm or falling threshold alarm or both.
This entry will exist forever	The lifespan of this alarm entry which can be forever or a specified period of time.
Latest value : 0	The value of the latest sampling.

display rmon statistics

Syntax

display rmon statistics [*port-num*]

View

All views

Parameter

port-num: Ethernet port number.

Description

Use the **display rmon statistics** command to display RMON statistics.

The displayed information includes collision, CRC (Cyclic Redundancy Check) and queue, undersized or oversized packet, timeout, fragment, broadcast, multicast, unicast, and bandwidth utility.

Related command: **rmon statistics.**

Example

Show RMON statistics.

```
<SW4500>display rmon statistics Ethernet 1/0/1
Statistics entry 1 owned by 3Com is VALID.
   Interface : Ethernet1/0/1<ifEntry.642>
   Received  :
   octets              :0         , packets          :0
   broadcast packets   :0         , multicast packets:0
   undersized packets  :0         , oversized packets:0
   fragments packets   :0         , jabbers packets  :0
   CRC alignment errors:0         , collisions       :0
   Dropped packet (insufficient resources):0
   Packets received according to length (octets):
   64     :0         ,  65-127  :0         ,  128-255  :0
   256-511:0         ,  512-1023:0         ,  1024-1518:0
```

Table 45 Output description of the display rmon statistics command

Field	Description
Interface	Port
3Com	Owner
VALID	The entry corresponding to the index is valid
octets	Received/Sent octets in sampling time
packets	Packets received/sent in sampling time
broadcast packets	Number of broadcast packets
multicast packets	Number of multicast packets
undersized packets	Number of undersized packets
oversized packets	Number of oversized packets
fragments packets	Number of undersized and CRC error packets
jabbers	Number of oversized and CRC error packets
CRC alignment errors	Number of CRC error packets
collisions	Number of collision packets
Dropped packet (insufficient resources)	Dropping packet events

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

Parameter

entry-number: Number of the entry to be added/deleted, ranging from 1 to 65535.

alarm-variable: Specifies the alarm variable with a character string, ranging from 1 to 256, in the OID dotted format, like 1.3.6.1.2.1.2.1.10.1 (or ifInOctets.1).

sampling-time: Specifies the sampling interval, ranging from 5 to 65535 (measured in seconds).

delta: Sampling type is delta.

absolute: Sampling type is absolute.

rising-threshold ***threshold-value1:*** Rising threshold, ranging from 0 to 2147483647.

event-entry1: Event number corresponding to the upper limit of threshold, ranging from 0 to 65535.

falling-threshold *threshold-value2*: Falling threshold, ranging from 0 to 2147483647.

event-entry2: Event number corresponding to the falling threshold, ranging from 0 to 65535.

owner *text*: Specifies the creator of the alarm. Length of the character string ranges from 1 to 127.

Description

Use the **rmon alarm** command to add an entry to the alarm table. Use the **undo rmon alarm** command to delete an entry from this table.

In this way, the alarm event can be triggered in the abnormal situations and then decides to log and send trap to the NM station.

Example

Delete the information of entry 15 from the alarm table.

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]undo rmon alarm 15
[SW4500]
```

rmon event

Syntax

rmon event *event-entry* [description *string*] { log | trap *trap-community* | log-trap *log-trapcommunity* | none } [owner *rmon-station*]

undo rmon event *event-entry*

View

System view

Parameter

event-entry: Number of the entry to be added/deleted, ranging from 1 to 65535.

description *string*: Event description. Length of the character string ranges from 1 to 255.

log: Log event.

trap: Trap event.

trap-community: The community of the Network Management station that the trap message is sent to.

log-trap: Log and trap event.

log-trapcommunity: The community of the Network Management station that the trap message is sent to.

none: neither log nor trap event.

owner *rmon-station:* Name of the network management station that creates this entry. The length of the character string ranges from 1 to 127.

Description

Use the **rmon event** command to add an entry to the event table. Use the **undo rmon event** command to delete an entry from this table.

Event management of RMON defines the way to deal with event number and event-log, send trap message or log while sending trap message. In this way, alarm events may obtain corresponding treatment

Example

Add the entry 10 to the event table and mark it as log event.

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]rmon event 10 log
[SW4500]
```

rmon history

Syntax

rmon history *entry-number* buckets *number* interval *sampling-interval* [owner *text-string*]

undo rmon history *entry-number*

View

Ethernet port view

Parameter

entry-number: Number of the entry to be added/deleted, ranging from 1 to 65535.

buckets *number*: Capacity of the history table corresponding to the control line.

interval *sampling-interval*: Sampling interval, ranging from 5 to 3600 (measured in seconds).

owner *text-string*: Creator of the line. Length of the character string ranges from 1 to127.

Description

Use the **rmon history** command to add an entry to the history control table. Use the **undo rmon history** command to delete an entry from history control table.

Perform this command to sample, set sample parameter (sample time interval) and storage amounts for a port. RMON will periodically perform data collection and save for query on this port. Sample information includes utility, error number and total packet number.

Example

Delete the entry 15 from the history control table.

```
<SW4500SW4500>system-view
System View: return to User View with Ctrl+Z.
```

```
[SW4500]interface Ethernet1/0/1
[SW4500-Ethernet1/0/1]undo rmon history 15
[SW4500-Ethernet1/0/1]
```

rmon prialarm

Syntax

rmon prialarm ***entry-number alarm-var*** **[** ***alarm-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

Parameter

entry-number: Specifies the entry number, ranging from 1 to 65535.

alarm-var: Specifies the alarm variable, which can be an arithmetic expression of several integer MIB node instances. The node can be OID in dotted notation.

alarm-des: Specifies the alarm description with a length ranging from 0 to 0-127;

sampling-timer: Sets the sampling interval, ranging from 10 to 65535 and measured in seconds.

delta | **absolute** | **changeratio:** Specifies the sampling type as delta ratio or absolute ratio.

threshold-value1: Rising threshold value, specified with a number greater than 0.

event-entry1: Corresponding event number to the upper limit threshold value, ranging from 0 to 65535.

threshold-value2: Falling threshold value, specified with a number greater than 0.

event-entry2: Event number corresponding to the falling threshold, ranging from 0 to 65535.

forever | **cycle** ***cycle-period:*** Specifies the type of the alarm instance line.

cycle-period specifies the functional cycle of the instance.

owner ***text*:** Specifies the creator of the line. Length of the character string ranges from 1 to 127.

Description

Use the **rmon prialarm** command to add an entry to the extended RMON alarm table. Use the **undo rmon prialarm** command to delete an entry from the extended RMON alarm table.

The number of instances can be created in the table depends on the hardware resource of the product.

Example

Delete line 10 from the extended RMON alarm table.

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]undo rmon prialarm 10
[SW4500]
```

rmon statistics

Syntax

rmon statistics ***entry-number*** **[owner** ***text-string*** **]**

undo rmon statistics ***entry-number***

View

Ethernet port view

Parameter

entry-number: Number of the entry to be added/deleted, ranging from 1 to 65535.

owner ***text-string:*** Creator of the entry. Length of the character string ranges from 1 to127.

Description

Use the **rmon statistics** command to add an entry to the statistic table. Use the **undo rmon statistics** command to delete an entry from statistic table.

RMON statistic management concerns the statistics and monitoring of the usage and error on a port. Statistics includes collision, CRC (Cyclic Redundancy Check) and queue, undersized or oversized packet, timeout, fragment, broadcast, multicast, unicast, and bandwidth utility.

Example

Add the statistics of Ethernet 1/0/1to entry 20 of the statistics table.

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]interface Ethernet1/0/1
[SW4500-ethernet1/0/1]rmon statistics 20
[SW4500-ethernet1/0/1]
```

NTP Configuration Commands

To protect unused sockets against attacks by malicious users and improve security, the Switch 4500 Family provides 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:

- Execute either **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 to enable the NTP feature and open UDP port 123 at the same time.
- Use the **undo** form of one of the above six commands to disable all implementation modes of the NTP feature and close UDP port 123 at the same time.

display ntp-service sessions

Syntax

display ntp-service sessions [verbose]

View

Any view

Parameter

verbose: Displays detailed NTP session information.

Description

Use the **display ntp-service sessions** command to display the information about all the sessions maintained by local NTP services. If you do not specify the **verbose** keyword, the brief information about all the sessions is displayed.

A Switch 4500 attempts to establish a connection in all NTP implementation modes except the NTP server mode.

Example

View the status of all sessions maintained by NTP services.

```
<SW4500> display ntp-service sessions
     source  reference   stra reach  pollnowoffsetdelay disper
**************************************************************
[12345]1.1.1.1  127.127.1.03 377   512  178  0.040.1  22.8
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

Table 46 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
stra	Stratum of the clock of the synchronization source
reach	Indicates whether or not the synchronization source is reachable.
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	Clock offset
delay	Network delay

Table 46 Description on the fields of the display ntp-service sessions command

disper	Maximum offset of the local clock relative to the reference clock

display ntp-service status

Syntax

display ntp-service status

View

Any view

Parameter

None

Description

Use the **display ntp-service status** command to display the status of NTP services.

Example

```
# View the status of the local NTP service.
<SW4500> display ntp-service status
 Clock status: unsynchronized
 Clock stratum: 16
 Reference clock ID: none
 Nominal frequency: 100.0000 Hz
 Actual frequency: 100.0000 Hz
 Clock precision: 2^17
 Clock offset: 0.0000 ms
 Root delay: 0.00 ms
 Root dispersion: 0.00 ms
 Peer dispersion: 0.00 ms
 Reference time: 00:00:00.000 UTC Jan 1 1900(00000000.00000000)
```

Table 47 Description on fields of the display ntp-service status command

Field	Description
Clock status	Status of the local clock
Clock stratum	Stratum of the local clock
Reference clock ID	Address of the remote server or ID of the reference clock after the local system is synchronized to a remote NTP server or a reference clock
Nominal frequency	Nominal frequency of the local clock
Actual frequency	Actual frequency of the local clock
Clock precision	Precision of the local clock
Clock offset	Offset of the local clock relative to the NTP server
Root delay	Roundtrip delay between the local clock and the primary reference clock
Root dispersion	Maximum dispersion of the local clock relative to the primary reference clock
Peer dispersion	Maximum dispersion of the remote NTP server

Table 47 Description on fields of the display ntp-service status command

Field	Description
Reference time	Reference timestamp

display ntp-service trace

Syntax

```
display ntp-service trace
```

View

Any view

Parameter

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 device to the reference clock source.

Example

View the brief information of each NTP time server along the time synchronization chain from the local device to the reference clock source.

```
<SW4500> 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 Reciever'
```

The above information displays the time synchronization chain of server4: serve4 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

Parameter

peer: Allows time request and query on the local NTP server. The local clock can also be synchronized to the remote server.

server: Allows time request and query on the local NTP server. The local clock cannot be synchronized to the remote server.

synchronization: Allows only time request on the local NTP server.

query: Allows only query on the local NTP server.

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 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 to the local NTP server is peer.

The ntp-service access command only provides a minimal degree of security measure. A more secure way is to perform identity authentication.

The right of a received access request is matched from the highest to the lowest in order of peer, server, synchronization, and query.

Example

Configure the peer in ACL 2076 to have the full access right to the local NTP server, including time request, query control, and time synchronization.

```
<SW4500> system-view
System View: return to User View with Ctrl+Z.
[SW4500] ntp-service access peer 2076
```

Configure the peer in ACL 2028 to have the right to access and query the local NTP server.

```
<SW4500> system-view
System View: return to User View with Ctrl+Z.
[SW4500] ntp-service access server 2028
```

ntp-service authentication enable

Syntax

```
ntp-service authentication enable
undo ntp-service authentication enable
```

View

System view

Parameter

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.

Example

Enable the NTP authentication.

```
<SW4500> system-view
System View: return to User View with Ctrl+Z.
[SW4500] 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

Parameter

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 **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.

Example

Configure an MD5 authentication key, with the key ID being 10 and the key being BetterKey.

```
<SW4500> system-view
System View: return to User View with Ctrl+Z.
[SW4500] 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

Parameter

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 switch operates in the broadcast client mode.

Example

Configure the switch to operate in the broadcast client mode and receive NTP broadcast messages through Vlan-interface1.

```
<SW4500> system-view
System View: return to User View with Ctrl+Z.
[SW4500] interface Vlan-interface1
[SW4500-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

Parameter

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 Ethernet switch operates in the NTP broadcast server mode.

Example

Configure the switch to send NTP broadcast messages through Vlan-interface1 and use authentication key 4 for encryption, and set the NTP version number to 3.

```
<SW4500> system-view
System View: return to User View with Ctrl+Z.
[SW4500] interface Vlan-interface 1
[SW4500-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

Parameter

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 enable the interface to receive NTP messages.

By default, the interface can receive NTP messages.

Example

Disable Vlan-interface1 from receiving NTP messages.

```
<SW4500> system-view
System View: return to User View with Ctrl+Z.
[SW4500] interface Vlan-interface 1
[SW4500-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

Parameter

number: Maximum number of the 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 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.

Example

Set the maximum number of dynamic NTP sessions that can be established locally to 50.

```
<SW4500> system-view
System View: return to User View with Ctrl+Z.
[SW4500] 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

Parameter

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 Ethernet switch operates in the NTP multicast client mode.

Example

Configure the switch to receive NTP multicast messages through Vlan-interface1, with the multicast IP address being 224.0.1.1.

```
<SW4500> system-view
System View: return to User View with Ctrl+Z.
[SW4500] interface Vlan-interface 1
[SW4500-Vlan-interface1] ntp-service multicast-client 224.0.1.1
```

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

Parameter

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 u**ndo ntp-service multicast-server** command to remove the configuration.

By default, no Ethernet switch operates in multicast server mode.

Example

Configure the switch to send NTP multicast messages through Vlan-interface1, and set the multicast group address to 224.0.1.1, keyid to 4, and the NTP version number to 3.

```
<SW4500> system-view
System View: return to User View with Ctrl+Z.
[SW4500] interface Vlan-interface 1
[SW4500-Vlan-interface1]ntp-service multicast-server 224.0.1.1
authentication-keyid 4 version 3
```

ntp-service reliable authentication-keyid

Syntax

ntp-service reliable authentication-keyid *key-id*
undo ntp-service reliable authentication-keyid *key-id*

View

System view

Parameter

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. If authentication is enabled, a client can only be synchronized to a server that can provide a trusted key.

Use the **undo ntp-service reliable authentication-keyid** command to remove the configuration.

By default, no trusted authentication key is configured.

Example

Enable NTP authentication. The encryption algorithm is MD5, the key ID is 37, and the trusted key is **BetterKey**.

```
<SW4500> system-view
System View: return to User View with Ctrl+Z.
[SW4500] ntp-service authentication enable
[SW4500] ntp-service authentication-keyid 37 authentication-mode md5
BetterKey
[SW4500] 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

Parameter

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 device 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.

Example

Specify the source IP addresses of all sent NTP messages as the IP address of Vla-interface1.

```
<SW4500> system-view
System View: return to User View with Ctrl+Z.
[SW4500] 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

Parameter

remote-ip: IP address of the NTP peer. This argument cannot be a broadcast address, a multicast address, or the IP address of the local reference clock.

peer-name: 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. You do not need to configure authentication-keyid key-id if authentication is not required.

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.

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 be an active NTP peer.

Use the **undo ntp-service unicast-peer** command to remove the configuration.

By default, the local Ethernet switch is not configured as an active NTP peer.

If you use remote-ip to specify a remote server as the peer of the local Ethernet switch, the local switch operates in the active peer mode. In this case, the local Ethernet switch and the remote server can be synchronized to each other.

Example

Configure the local peer to obtain time information from the peer with the IP address 128.108.22.44 and also to provide time information to the remote peer. Set the NTP version number to 3. The source IP address of NTP messages is the IP address of Vlan- interface1.

```
<SW4500> system-view
System View: return to User View with Ctrl+Z.
[SW4500] 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

Parameter

remote-ip: IP address of an NTP server. This argument cannot be a broadcast address, multicast group address, or IP address of a reference 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. You do not need to configure authentication-keyid key-id if authentication is not required.

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 device 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 Ethernet switch operates in the NTP client mode.

The remote server specified by remote-ip serves as the NTP server and the local Ethernet switch serves as the NTP client. The client can be synchronized to the server while the server cannot be synchronized to the client.

Example

```
# Configure the local device to be synchronized to the NTP server
with the IP address 128.108.22.44, and set the version number to 3.
<SW4500> system-view
System View: return to User View with Ctrl+Z.
[SW4500] ntp-service unicast-server 128.108.22.44 version 3
```

SSH Terminal Service Configuration Commands

This section describes the SSH configuration commands available on your Switch 4500.

debugging ssh server

Syntax

debugging ssh server { VTY *vty-num* | all}

undo debugging ssh server {VTY *vty-num* | all}

View

User View

Parameter

vty-num: SSH channel to be debugged whose value is dictated by VTY numbers ranging from 0 to 4.

all: All SSH channels

Description

Use the **debugging ssh server** command to send information regulated by the SSH2.0 protocol, such as the negotiation procedure, to the information center in the format of debugging information. You can also use it to debug a user interface individually.

Use the **undo debugging ssh server** command to disable debugging.

By default, the debugging is disabled.

Related commands: **ssh server authentication-retries**, **ssh server rekey-interval**, **ssh server timeout**.

Example

To print debugging information in running SSH, enter the following:

```
<SW4500>debug ssh server all
<SW4500>term debug
% Current terminal debugging is on

<SW4500>
*0.1303820 SW4500 SSH/8/debugging_msg_send:- 1 -SSH_VERSION_SEND message sent
 on VTY -2117588440
*0.1303929 SW4500 SSH/8/msg_rcv_vty:- 1 -SSH_VERSION_RECEIVE message received
 on VTY 2
*0.1317315 SW4500 SSH/8/msg_rcv_vty:- 1 -SSH_MSG_REQUEST_PTY message received
 on VTY 2
*0.1317412 SW4500 SSH/8/msg_rcv_vty:- 1 -SSH_MSG_START_SHELL message received
 on VTY 2
%Apr  2 00:16:57:529 2000 SW4500 SHELL/5/LOGIN:- 1 - sting(158.101.28.103) in
 unit1 login
*0.1321800 SW4500 SSH/8/msg_rcv_vty:- 1 -SSH_MSG_CHANNEL_DATA message receive
d on VTY 2
*0.1444455 SW4500 SSH/8/debugging_msg_send:- 1 -SSH_VERSION_SEND message sent
on VTY -2117588440
*0.1444572 SW4500 SSH/8/msg_rcv_vty:- 1 -SSH_VERSION_RECEIVE message received
on VTY 3
```

```
*0.1481894 SW4500 SSH/8/debugging_msg_send:- 1 -SSH2_MSG_USERAUTH_SUCCESS
message sent on VTY 3
*0.1481995 SW4500 SSH/8/msg_rcv_vty:- 1 -SSH_MSG_REQUEST_PTY message received
on VTY 3
*0.1482095 SW4500 SSH/8/msg_rcv_vty:- 1 -SSH_MSG_START_SHELL message received
on VTY 3
%Apr  2 00:19:42:212 2000 SW4500 SHELL/5/LOGIN:- 1 - Bono(158.101.28.103) in
unit1 login
*0.1484308 SW4500 SSH/8/msg_rcv_vty:- 1 -SSH_MSG_CHANNEL_DATA message
received on VTY 3
*0.1485966 SW4500 SSH/8/msg_rcv_vty:- 1 -SSH_MSG_CHANNEL_DATA message
received on VTY 3
*0.1493206 SW4500 SSH/8/msg_rcv_vty:- 1 -SSH_MSG_CHANNEL_DATA message
received on VTY 3
*0.1493326 SW4500 SSH/8/msg_rcv_vty:- 1 -SSH_MSG_CHANNEL_DATA message
received on VTY 3
*0.1493518 SW4500 SSH/8/msg_rcv_vty:- 1 -SSH_MSG_CHANNEL_DATA message
received on VTY 3
*0.1494015 SW4500 SSH/8/msg_rcv_vty:- 1 -SSH_MSG_CHANNEL_DATA message
received on VTY 3
*0.1502822 SW4500 SSH/8/msg_rcv_vty:- 1 -SSH_MSG_CHANNEL_DATA message
received on VTY 2
*0.1502918 SW4500 SSH/8/msg_rcv_vty:- 1 -SSH_MSG_CHANNEL_DATA message
received on VTY 2
*0.1503031 SW4500 SSH/8/msg_rcv_vty:- 1 -SSH_MSG_CHANNEL_DATA message
received on VTY 2
*0.1503185 SW4500 SSH/8/msg_rcv_vty:- 1 -SSH_MSG_CHANNEL_DATA message
received on VTY 2
*0.1503984 SW4500 SSH/8/msg_rcv_vty:- 1 -SSH_MSG_CHANNEL_DATA message
received on VTY 2
%Apr  2 00:20:04:219 2000 SW4500 SHELL/5/LOGOUT:- 1 - sting(158.101.28.103)
in unit1 logout
<SW4500>undo debug ssh server all
```

display rsa local-key-pair public

Syntax

display rsa local-key-pair public

View

All views

Parameter

None

Description

Use the **display rsa local-key-pair public** command to display the public key of the server's host key pair and server key pair. If no key has been created, you will see a prompt similar to the following: "RSA keys not found".

Related command: **rsa local-key-pair create**.

Example

To display local key pair and public key of the server, enter the following:

```
<SW4500>display rsa local-key-pair public

=====================================================
Time of Key pair created: 21:59:43  2000/04/02
```

```
Key name: SW4500_Host
Key type: RSA encryption Key
=================================================
Key code:
308188
  028180
    A768F212 CDF98303 7D641E14 89BC50AC 6B0B1B82
    9EA5E2A1 66164625 A092CA18 7CCBF3BC 74BA2A6F
    9A5783F9 D2DD4BE7 F65296BE E8D3AC9C EE35A380
    0F626AFA E1B6B9B4 84F25041 EEE8B407 49D4AF18
    3D4FB033 D4365AE4 58483507 664D5AE5 0122D602
    19E47685 DD49481B 0D443A73 34A0EA6B 24A66472
    0BB4A01A 509926D3
  0203
    010001

 Host public key for PEM format code:
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1yc2EAAAADAQABAAAAgQCnaPISzfmDA31kHhSJvFCsawsbgp6l4qFm
FkYloJLKGHzL87x0uipvmleD+dLdS+f2Upa+6NOsnO41o4APYmr64ba5tITyUEHu
6LQHSdSvGD1PsDPUNlrkWEg1B2ZNWuUBItYCGeR2hd1JSBsNRDpzNKDqaySmZHIL
tKAaUJkm0w==
---- END SSH2 PUBLIC KEY ----

Public key code for pasting into OpenSSH authorized_keys file :
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQCnaPISzfmDA31kHhSJvFCsawsbgp6l4qFmFkYl
oJLK
GHzL87x0uipvmleD+dLdS+f2Upa+6NOsnO41o4APYmr64ba5tITyUEHu6LQHSdSvGD1P
sDPUNlrkWEg1
B2ZNWuUBItYCGeR2hd1JSBsNRDpzNKDqaySmZHILtKAaUJkm0w== rsa-key

<SW4500>
```

display rsa peer-public-key

Syntax

display rsa peer-public-key [brief | name *keyname*]

View

All views

Parameter

brief: Displays brief information about all client public keys.

***keyname*:** Specifies the public key name of the client to be displayed which is a string consisting of 1 to 64 characters.

Description

Use the **display rsa peer-public-key** command to display the public key of RSA key pair specified by the client. If you do not specify the ***keyname*** argument, all public keys will be displayed.

Related command: **rsa local-key-pair create**.

Example

To display all of the RSA public keys currently configured, enter the command **display rsa peer-public-key** .

```
<SW4500>display rsa peer-public-key
Address         Bits   Name
                 1023   abcd
                 1024   hq
```

To display information about the public key of the client named candy2, enter the following:

```
[SW4500]display rsa peer-public-key name candy2

=====================================
    Key name: candy2
    Key address:
=====================================
Key Code:
308186
  028180
    5E12F775 653A1112 EDAD305F 3E53EBBD E8C66CA8 9AE79A23 D142CB38
55F85E06
    8538FFEF 5D6F3F83 E529F336 5F492650 22356D32 9D4C6414 8AF36DA8
7DAEDB77
    FFF8B17C 34317BA0 6F5A40B0 1A62D1ED C6F18DC2 9EAB5B95 510FFEA3
D2AC6F10
    BB3CE5EC E2142587 A541E094 240A97BF FA38F68B 45241B46 E10F8BDE
21BF734F
  0201
    25
[SW4500]
```

display ssh server

Syntax

display ssh server { status | session }

View

All views

Parameter

status: Displays the SSH status information

session: Displays the SSH session information

Description

Use the **display ssh server** command to display the status information or session information of an SSH server.

Related commands: **ssh server authentication-retries**, **ssh server rekey-interval**, **ssh server timeout, ssh server compatible_ssh1x enable**

Example

To display the status information of the SSH server, enter the following:

```
[SW4500]display ssh server status
SSH version : 2.0
SSH connection timeout : 60 seconds
SSH server key generating interval : 0 hours
SSH Authentication retries : 3 times
SFTP Server: Disable
```

To display SSH sessions:

```
[SW4500]display ssh server session
 Conn    Ver    Encry     State      Retry     Username
 VTY 3   2.0    AES       started      0             Bono
```

display ssh user-information

Syntax

display ssh user-information [*username*]

View

All views

Parameter

***username*:** A valid SSH username which is a string consisting of 1 to 80 characters.

Description

Use the **display ssh user-information** command to display information about the current SSH user, including username, authentication mode, corresponding key name and the types of authorized services. If you specify ***username*** in the command, the user information about the specified username will be displayed.

Related commands: **ssh user username assign rsa-key**, **ssh user username authentication-type**.

Example

To display the current user information, enter the following:

```
[SW4500]display ssh user-information
 Username    Authentication-type  User-public-key-name    Service-type
 sting         rsa                sw4500sting              stelnet|sftp
 client002     password           sw4500client002          stelnet|sftp
 admin         password           null                     stelnet|sftp
 doll          password           null                     stelnet
 client001     password           null                     stelnet
 kathis        rsa                candy2                   stelnet|sftp
 bono          password-publickey sw7750                   stelnet|sftp
 client003     rsa                passphrase               stelnet|sftp
 client10      password           null                     stelnet
```

peer-public-key end

Syntax

peer-public-key end

View

Public key view

Parameter

None

Description

Use the **peer-public-key end** command to exit from the public key view and return to the system view.

Related commands: **rsa peer-public-key**, **public-key-code begin**.

Example

To quit public key view, enter the following:

```
<SW4500>system-view
System View: return to User View with Ctrl+Z.
[SW4500]rsa peer-public-key 3COM003
[SW4500-rsa-public-key]peer-public-key end
[SW4500]
```

protocol inbound

Syntax

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

View

VTY user interface view

Parameter

all: Supports all protocols, including Telnet and SSH.

ssh: Supports the SSH protocol only.

telnet: Supports the Telnet protocol only.

Description

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

By default, all protocols are supported.

The configuration takes effect at the next login. After enabling SSH you cannot login through SSH if the client RSA key is not configured.

If the supported protocol configured in the user interface is SSH, you must ensure you configure the corresponding authentication mode to **authentication-mode scheme** *(using AAA authentication mode).*

If the authentication mode is configured as **authentication-mode password** *or* **authentication-mode none**, *the configuration of* **protocol inbound ssh** *will fail. However, if a user interface is configured to support the SSH protocol, you will be unable to configure* **authentication-mode password** *and* **authentication-mode none**.

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

Example

To set VTY 0 to 4 to support SSH protocol only, enter the following:

```
[SW4500]user-interface vty 0 4
```

```
[SW4500-ui-vty0-4]protocol inbound ssh
```

To disable the Telnet function of VTY 0 and make it support SSH only:

```
[SW4500]user-interface vty 0
[SW4500-ui-vty0]protocol inbound ssh
```

public-key-code begin

Syntax

public-key-code begin

View

Public key edit view

Parameter

None

Description

Use the **public-key-code begin** command to enter the public key edit view and input the public key of the client.

When inputting the public key, you may type spaces between the characters (the system will delete the spaces automatically), or press *Enter* and continue to input the key. Note that the public key must be a hexadecimal string coded in the public key format and is randomly generated by the SSH 2.0-enabled client software.

Related commands: **rsa peer-public-key**, **public-key-code end**.

Example

To enter the public key edit view and input the key, enter the following:

```
[SW4500]rsa peer-public-key quidway003
[SW4500-rsa-public-key]public-key-code begin
[SW4500-key-code]308186028180739A291ABDA704F5D93DC8FDF84C427463
[SW4500-key-code]1991C164B0DF178C55FA833591C7D47D5381D09CE82913
[SW4500-key-code]D7EDF9C08511D83CA4ED2B30B809808EB0D1F52D045DE4
[SW4500-key-code]0861B74A0E135523CCD74CAC61F8E58C452B2F3F2DA0DC
[SW4500-key-code]C48E3306367FE187BDD944018B3B69F3CBB0A573202C16
[SW4500-key-code]BB2FC1ACF3EC8F828D55A36F1CDDC4BB45504F020125
[SW4500-key-code]public-key-code end
[SW4500-rsa-public-key]
```

public-key-code end

Syntax

public-key-code end

View

Public key edit view

Parameter

None

Description

Use the **public-key-code end** command to return from the public key edit view to the public key view and save the public key entered.

After this command is performed to end the public key edit procedure, the system will check the validity of the key before saving the input public key. If the public key string contains any illegal character, the system will prompt the failure of the configuration and the configured key will be discarded; otherwise, the key is valid and will be saved to the user public key list.

Related command: **rsa peer-public-key**, **public-key-code begin**.

Example

To exit the public key edit view and save the configuration, enter the following:

```
[SW4500-rsa-key-code]public-key-code end
[SW4500-rsa-public-key]
```

rsa local-key-pair create

Syntax

rsa local-key-pair create

View

System view

Parameter

None

Description

Use the **rsa local-key-pair create** command to generate the RSA key pair (including the host key and server key) of the server.

When configuring by this command, if the RSA key pair already exists, you receive get a warning asking if you want to replace the existing one. Note that the host key and the server key must have a difference of 128 bits at least, and that the minimum and maximum lengths for the host key and the server key are 512 bits and 2048 bits respectively.

When the client version is SSH 2.0, the RSA key of the SSH server must be no less than 1024 bits in length, otherwise the authentication will fail

Generating the RSA key pair of the server is the first step to perform after SSH login. You will not need to generate the RSA key pair after rebooting the Switch.

Related command: **rsa local-key-pair destroy**.

Example

To generate the local RSA key pair, enter the following:

```
[SW4500]rsa local-key-pair create
[SW4500]rsa local-key-pair create
The key name will be: SW4500_Host
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 = 512]:1024
Generating keys...
.................................................++++++
.............................++++++
```

rsa local-key-pair destroy

Syntax

rsa local-key-pair destroy

View

System view

Parameter

None

Description

Use the **rsa local-key-pair destroy** command to destroy all the RSA key pairs of the server, including the host keys and server keys.

Related command: **rsa local-key-pair create**.

Example

To destroy all the RSA key pairs of the server, enter the following:

```
[SW4500]rsa local-key-pair destroy
% The name for the keys which will be destroyed is SW4500_Host .
% Confirm to destroy these keys? [Y/N]:y
```

rsa peer-public-key

Syntax

rsa peer-public-key ***key-name***

View

System view

Parameter

***key-name*:** The name of the public key which is a string consisting of 1 to 64 characters.

Description

Use the **rsa peer-public-key** command to enter the public key view.

When using this command together with the public-key-code begin command to configure the public key at the client, which is generated randomly by the client program supporting SSH1.5.

Related commands: **public-key-code begin**, **public-key-code end**.

Example

To enter the public key view name 3Com002, enter the following:

```
[SW4500]rsa peer-public-key 3COM002
[SW4500-rsa-public-key]
```

ssh server authentication-retries

Syntax

ssh server authentication-retries ***times***
undo ssh server authentication-retries

View

System view

Parameter

***times*:** Specifies authentication retry times, in the range of 1~5.

Description

Use the **ssh server authentication-retries** command to define SSH authentication retry times value, which takes effect at next logon.

Use the **undo ssh server authentication-retries** command to restore the default retry value.

By default, it is 3.

Related command: **display ssh server**.

Example

To define the authentication retry times value as 4, enter the following:

```
[SW4500]ssh server authentication-retries 4
```

ssh server timeout

Syntax

ssh server timeout ***seconds***

undo ssh server timeout

View

System view

Parameter

***seconds*:** Specifies the login timeout (in seconds) in the range 1 to 120.

Description

Use the **ssh server timeout** command to set the authentication timeout of SSH connections.

Use the **undo ssh server timeout** command to restore the default value.

By default, the timeout value is 60 seconds.

Related command: **display ssh server**. **status**

Example

To define the registration timeout value as 80 seconds, enter the following:

```
[SW4500]ssh server timeout 80
```

ssh user assign rsa-key

Syntax

ssh user ***username*** **assign rsa-key** ***keyname***

undo ssh user ***username*** **assign rsa-key**

View

System view

Parameter

***username*:** A valid SSH username, which is a string consisting of 1 to 80 characters.

***keyname*:** A name of the client public key which is a string consisting of 1 to 54 characters.

Description

Use the **ssh user username assign rsa-key** command to assign an existing public key for the specified SSH user.

Use the **undo ssh user username assign rsa-key** command to delete the association.

For a user who has been associated with a public key, the command associates him/her with the new public key.

The new public key takes effect at the next login.

Related command: **display ssh user-information**.

Example

To associate the key 1 with jsmith, enter the following:

```
[SW4500]ssh user jsmith assign rsa-key key1
```

ssh user authentication-type

Syntax

ssh user *username* authentication-type { password | rsa | password-publickey | all}

undo ssh user *username* authentication-type

View

System View

Parameter

***username*:** A valid SSH username which is a string consisting of 1 to 80 characters.

password: Forces the user's authentication mode to password authentication.

rsa: Forces the user's authentication mode to RSA public key authentication.

password-publickey: Forces the user's authentication mode to password authentication plus RSA public key authentication.

all: Specifies authentication type as password and RSA.

Description

Use the **ssh user username authentication-type** command to define authentication type for a designated user.

Use the **undo ssh user username authentication-type** command to restore the default mode in which logon fails.

By default, user cannot logon to the Switch through SSH or TELNET, you need to specify the authentication type for a new user. The new configuration takes effects at the next logon.

Related commands: **display ssh user-information**.

Example

To specify jsmith's authentication type as password, enter the following:

```
[SW4500]ssh user jsmith authentication-type password
```

SSH Client Configuration Commands

This section describes the SSH client configuration commands available on your Switch 4500.

display ssh server-info

Syntax

display ssh server-info

View

Any View

Parameter

None

Description

Use the **display ssh server-info** command to view the corresponding relationship between the client's public key of the servers and servers.

Example

To display the corresponding relationship between the client's servers and public keys, enter the following:

```
[SW4500]display ssh server-info

Server Name(IP)                 Server public key name
_____________________________________________________

192.168.0.1                     abc_key01
192.168.0.2                     abc_key02
```

peer-public-key end

Syntax

peer-public-key end

View

Public key view

Parameter

None

Description

Use the peer-public-key end command to exit from the public key view and return to the system view.

Related commands: **rsa peer-public-key, public-key-code begin**.

Example

To exit the public key view, enter the following:

```
[SW4500]rsa peer-public-key SW4500003
[SW4500-rsa-public-key]peer-public-key end
[SW4500]
```

public-key-code begin

Syntax

public-key-code begin

View

Public key view

Parameter

None

Description

Use the **public-key-code begin** command to enter the public key edit view and input the public key of the server.

When inputting the public key, you may type spaces between the characters (the system will delete the spaces automatically), or press <Enter> and then continue to input the key.

The public key must be a hexadecimal string coded in the public key format. The public key of the server is generated by the rsa local-key-pair create command.

Related commands: **rsa peer-public-key, public-key-code end**

Example

To enter the public key edit view and input the public key of the server, enter the following:

```
[SW4500]rsa peer-public-key SW4500003
[SW4500-rsa-public-key]public-key-code begin
[SW4500-key-code]308186028180739A291ABDA704F5D93DC8FDF84C427463
[SW4500-key-code]1991C164B0DF178C55FA833591C7D47D5381D09CE82913
[SW4500-key-code]D7EDF9C08511D83CA4ED2B30B809808EB0D1F52D045DE4
[SW4500-key-code]0861B74A0E135523CCD74CAC61F8E58C452B2F3F2DA0DC
[SW4500-key-code]C48E3306367FE187BDD944018B3B69F3CBB0A573202C16
```

```
[SW4500-key-code]BB2FC1ACF3EC8F828D55A36F1CDDC4BB45504F020125
[SW4500-key-code]public-key-code end
[SW4500-rsa-public-key]
```

public-key-code end

Syntax

public-key-code end

View

Public key edit view

Parameter

None

Description

Use the **public-key-code end** command to return from the public key edit view to the public key view and save the public key of the server entered.

After this command is performed to end the public key edit procedure, the system will check the validity of the key before saving the input public key. If the public key string contains any illegal character, the system will prompt the failure of the configuration and the configured key will be discarded; otherwise, the key is valid and will be saved.

Related commands: **rsa peer-public-key, public-key-code begin**

Example

To exit the public key edit view and save the public key of the server, enter the following:

```
[SW4500-rsa-key-code]public-key-code end
[SW4500-rsa-public-key]
```

quit

Syntax

quit

View

User View

Parameter

None

Description

Use the **quit** command to terminate the connection with the remote SSH server.

Example

To terminate the connection with the remote SSH server, enter the following:

```
<SW4500>quit
```

rsa peer-public-key

Syntax

rsa peer-public-key *key-name*

View

System View

Parameter

key-name: The name of the public key of the server, which is a string consisting of 1 to 64 characters.

Description

Use the **rsa peer-public-key** command to enter the public key view.

Performing this command, you can enter the public key view. Then you can use the **public-key-code begin** command to configure the public key of the server on the client. The public key of the server is generated by the **rsa local-key-pair create** command.

Related commands: **public-key-code begin, public-key-code end**

Example

To enter the public key view named SW4500002, enter the following:

```
[SW4500]rsa peer-public-key SW4500002
[SW4500-rsa-public-key]
```

ssh client assign rsa-key

Syntax

ssh client { *server-ip* | *server-name* } assign rsa-key *keyname*

undo ssh client server-ip assign rsa-key

View

System View

Parameter

server-ip: The IP address of the SSH server.

server-name: The name of the SSH server, which is a string consisting of 1 to 80 characters.

keyname: The name of the public key of the server, which is a string consisting of 1 to 64 characters.

Description

Use the **ssh client assign rsa-key** command to specify the public key of the server to connect with on the client, so that the client authenticates if the server is trustworthy.

Use the **undo ssh client assign rsa-key** command to cancel the specified relationship with the public key of the server.

Example

To specify abc as the public key name of the server with IP address 192.168.0.1 on the client, enter the following:

```
[SW4500]ssh client 192.168.0.1 assign rsa-key abc
```

ssh client first-time enable

Syntax

ssh client first-time enable

undo ssh client first-time

View

System View

Parameter

None

Description

Use the **ssh client first-time enable** command to set the SSH client to perform the first-time authentication of the SSH server to be accessed.

Use the **undo ssh client first-time** command to cancel the first-time authentication.

The first-time authentication means that when the SSH client accesses the server for the first time in the case that there is no local copy of the server's public key, the user can proceed to access the server and save a local copy of the server's public key; when the client accesses the server next time, it uses the saved public key to authenticate the server.

If the first-time authentication is not supported, when there is no local copy of the public key of the connected server, the client assumes that the server is illegal and will refuse to access the server. The user can save a copy of the server's public key locally by other means beforehand.

By default, the client perform the first-time authentication.

Example

To set the SSH client to perform the first-time authentication of the SSH server to be accessed, enter the following:

```
[SW4500]ssh client first-time enable
```

ssh2 Syntax

ssh2 { *host-ip* | *host-name* } [*port-num*] [prefer_kex { dh_group1 | dh_exchange_group }] [prefer_ctos_cipher { des | 3des | aes128 }] [prefer_stoc_cipher { des | 3des | aes128 }] [prefer_ctos_hmac { sha1 | sha1_96 | md5 | md5_96 }] [prefer_stoc_hmac { sha1 | sha1_96 | md5 | md5_96 }]

View

System View

Parameter

host-ip: IP address of the server.

host-name: The name of the server. It is a string with a length of 1 to 20 characters.

port-num: The port number of the server, ranging from 0 to 65535. By default, the port number is 22.

prefer_kex: Preferred key exchange algorithm, which can be one of the two algorithms.

dh_group1: Key exchange algorithm diffie-hellman-group1-sha1, which is the default algorithm.

dh_exchange_group: Key exchange algorithm diffie-hellman-group-exchange-sha1.

prefer_ctos_cipher: Preferred encryption algorithm from the client to the server. The default algorithm is aes128.

prefer_stoc_cipher: Preferred encryption algorithm from the server to the client. The default algorithm is aes128.

des: Encryption algorithm des_cbc.

3des: Encryption algorithm 3des_cbc.

aes128: Encryption algorithm aes_128.

prefer_ctos_hmac: Preferred HMAC algorithm from the client to the server. The default algorithm is sha1_96.

prefer_stoc_hmac: Preferred HMAC algorithm from the server to the client. 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 **ssh2** command to enable the connection between the SSH client and the server, and specify the preferred key exchange algorithm, encryption algorithm and HMAC algorithm of the client and the server.

Example

To log in to the remote SSH2 server with the IP address 10.214.50.51, and configure encryption algorithms as follows:

- Preferred key exchange algorithm: dh_exchange_group
- Preferred encryption algorithm from the client to the server: 3DES-CBC
- Preferred HMAC algorithm from the client to the server: HMAC-MD5
- Preferred encryption algorithm from the server to the client: AES-128
- Preferred HMAC algorithm from the server to the client: HMAC-SHA1-96

```
[SW4500]ssh2 10.214.50.51 prefer_kex dh_exchange_group
prefer_ctos_cipher 3des prefer_ctos_hmac md5
```

SFTP Server Configuration Commands

This section describes the SFTP server configuration commands available on your Switch 4500.

sftp server enable

Syntax

sftp server enable

undo sftp server

View

System View

Parameter

None

Description

Use the **sftp server enable** command to start the SFTP server.

Use the **undo sftp server** command to shutdown the SFTP server.

By default, the SFTP server is shutdown.

Example

To start the SFTP server, enter the following:

```
[SW4500]sftp server enable
```

To shutdown the SFTP server, enter the following:

```
[SW4500]undo sftp server
```

ssh user service-type

Syntax

ssh user *username* service-type { stelnet | sftp | all }

undo ssh user *username* service-type

View

System View

Parameter

username: Local username or username defined by the remote RADIUS/TACACS server. It is a string with a length of 1 to 80 characters.

stelnet: Specifies the service type as secure Telnet.

sftp: Specifies the service type as secure FTP.

all: Includes both stelnet and sftp service types.

Description

Use the **ssh user service-type** command to specify the service type for a particular user.

Use the **undo ssh user service-type** command to restore the default service type.

By default, the service type is **stelnet**.

Related command: **display ssh user-information**

Example

To specify the service type to be SFTP for user J Smith, enter the following:

```
[SW4500]ssh user jsmith service-type sftp
```

SFTP Client Configuration Commands

This section describes the SFTP client configuration commands available on your Switch 4500.

bye

Syntax

bye

View

SFTP Client View

Parameter

None

Description

Use the **bye** command to terminate the connection with the remote SFTP server and return to the system view.

This command has the same functionality as the **exit** and **quit** commands.

Example

To terminate the connection with the remote SFTP server, enter the following:

```
Sftp-client>bye
[SW4500]
```

cd

Syntax

cd [***remote-path*** **]**

View

SFTP Client View

Parameter

remote-path: The name of a path on the server.

Description

Use the **cd** command to change the current path on the SFTP server. If you do not specify the remote-path argument, the current path will be displayed.

Example

To change the current path to d:/temp, enter the following:

```
sftp-client>cd d:/temp
```

cdup

Syntax

cdup

View

SFTP Client View

Parameter

None

Description

Use the **cdup** command to change the current path to its upper directory.

Example

To change the current path to its upper directory, enter the following:

```
sftp-client>cdup
```

delete

Syntax

delete *remote-file*

View

SFTP Client View

Parameter

remote-file:The name of a file on the server.

Description

Use the **delete** command to delete the specified file from the server.

This command has the same functionality as the **remove** command.

Example

To delete the file temp.c from the server, enter the following:

```
sftp-client>delete temp.c
```

dir

Syntax

dir[*remote-path*]

View

SFTP client view

Parameter

remote-path:The name of the directory to view.

Description

Use the **dir** command to view the files in the specified directory.

If ***remote-path*** is not specified, the files in the current directory will be displayed.

This command has the same functionality as the **ls** command.

Example

To view the directory, flash:/, enter the following:

```
sftp-client>dir flash:/
-rwxrwxrwx   1 noone    nogroup       1759 Aug 23 06:52 vrpcfg.cfg
-rwxrwxrwx   1 noone    nogroup        225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup        283 Aug 24 07:39 pubkey1
-rwxrwxrwx   1 noone    nogroup        225 Sep 28 08:28 pub1
drwxrwxrwx   1 noone    nogroup          0 Sep 28 08:24 new1
drwxrwxrwx   1 noone    nogroup          0 Sep 28 08:18 new2
-rwxrwxrwx   1 noone    nogroup        225 Sep 28 08:30 pub2
```

exit

Syntax

exit

View

SFTP client view

Parameter

None

Description

Use the **exit** command to terminate the connection with the remote SFTP server and return to the System view.

This command has the same functionality as the **bye** and **quit** commands.

Example

To terminate the connection with the remote SFTP server, enter the following:

```
sftp-client>exit
[SW4500]
```

get

Syntax

get ***remote-file*** **[** ***local-file*** **]**

View

SFTP client view

Parameter

remote-file: The name of a file on the remote SFTP server.

local-file: The name of a local file.

Description

Use the **get** command to download a file from the remote server and save it locally.

By default, if no local file name is specified, it is assumed that the local file has the same name as the file on the SFTP server.

Example

To download file temp1.c and save it with name temp.c, enter the following

```
sftp-client>get temp1.c temp.c
```

help

Syntax

help [***command*** **]**

View

SFTP client view

Parameter

command: The name of a command.

Description

Use the **help** command to view the help information for SFTP client commands.

If the command argument is not specified, all command names will be displayed.

Example

To view the help information for the get command, enter the following:

```
sftp-client>help get
get remote-path [local-path]  Download file
Default local-path is the same with remote-path
```

ls Syntax

ls [*remote-path*]

View

SFTP client view

Parameter

remote-path: The name of the directory to view.

Description

Use the **ls** command to view the files in the specified directory.

If ***remote-path*** is not specified, the files in the current directory will be displayed.

This command has the same functionality as the **dir** command.

Example

To view the directory flash:/, enter the following:

```
sftp-client>ls flash:/
-rwxrwxrwx   1 noone    nogroup       1759 Aug 23 06:52 vrpcfg.cfg
-rwxrwxrwx   1 noone    nogroup        225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup        283 Aug 24 07:39 pubkey1
-rwxrwxrwx   1 noone    nogroup        225 Sep 28 08:28 pub1
drwxrwxrwx   1 noone    nogroup          0 Sep 28 08:24 new1
drwxrwxrwx   1 noone    nogroup          0 Sep 28 08:18 new2
-rwxrwxrwx   1 noone    nogroup        225 Sep 28 08:30 pub2
```

mkdir Syntax

mkdir *remote-path*

View

SFTP client view

Parameter

remote-path: The name of a directory on the remote SFTP server.

Description

Use the **mkdir** command to create a directory on the remote SFTP server.

Example

To create a directory test on the remote SFTP server, enter the following:

```
sftp-client>mkdir test
```

put

Syntax

put *local-file* [*remote-file*]

View

SFTP client view

Parameter

local-file: The name of a local file.

remote-file: The 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, if the name of the file on the remote server is not specified, it is assumed that the file on the remote server has the same name as the local file.

Example

To upload local file temp.c to the remote SFTP server and save it with the name temp1.c, enter the following:

```
sftp-client>put temp.c temp1.c
```

pwd

Syntax

pwd

View

SFTP client view

Parameter

None

Description

Use the **pwd** command to display the current directory on the SFTP server.

Example

To display the current directory on the SFTP server, enter the following:

```
sftp-client>pwd
flash:
```

quit

Syntax

quit

View

SFTP client view

Parameter

None

Description

Use the **quit** command to terminate the connection with the remote SFTP server and return to the System view.

This command has the same functionality as the **bye** and **exit** commands.

Example

To terminate the connection with the remote SFTP server, enter the following:

```
sftp-client>quit
[SW4500]
```

remove

Syntax

remove ***remote-file***

View

SFTP client view

Parameter

remote-file: The name of a file on the server.

Description

Use the **remove** command to delete the specified file from the server.

This command has the same functionality as the **delete** command.

Example

To delete the file temp.c from the server, enter the following:

```
sftp-client>remove temp.c
```

rename

Syntax

rename ***oldname newname***

View

SFTP client view

Parameter

oldname: Original file name.

newname: New file name.

Description

Use the **rename** command to change the name of the specified file on the SFTP server.

Example

To change the name of the file temp1 on the SFTP server to temp2, enter the following:

```
sftp-client>rename temp1 temp2
```

rmdir

Syntax

rmdir *remote-path*

View

SFTP client view

Parameter

remote-path: The name of a directory on the remote SFTP server.

Description

Use the **rmdir** command to delete the specified directory from the SFTP server.

Example

To delete the directory D:/temp1 from the SFTP server, enter the following:

```
sftp-client>rmdir D:/temp1
```

sftp

Syntax

sftp { *host-ip* | *host-name* } [*port-num*] [prefer_kex { dh_group1 | dh_exchange_group }] [prefer_ctos_cipher { des | 3des | aes128 }] [prefer_stoc_cipher { des | 3des | aes128 }] [prefer_ctos_hmac { sha1 | sha1_96 | md5 | md5_96 }] [prefer_stoc_hmac { sha1 | sha1_96 | md5 | md5_96 }]

View

System view

Parameter

host-ip: The IP address of the server.

host-name: The name of the server. It is a string with a length of 1 to 20 characters.

port-num: The port number of the server, ranging from 0 to 65535. By default, the port number is 22.

prefer_kex: Preferred key exchange algorithm, which can be either diffie-hellman-group1-sha1 or diffie-hellman-group-exchange-sha1.

dh_group1: Key exchange algorithm diffie-hellman-group1-sha1, which is default algorithm.

dh_exchange_group: Key exchange algorithm diffie-hellman-group-exchange-sha1.

prefer_ctos_cipher: Preferred encryption algorithm from the client to the server. The default algorithm is aes128.

prefer_stoc_cipher: Preferred encryption algorithm from the server to the client. The default algorithm is aes128.

des: Encryption algorithm des_cbc.

3des: Encryption algorithm 3des_cbc.

aes128: Encryption algorithm aes_128.

prefer_ctos_hmac: Preferred HMAC algorithm from the client to the server. The default algorithm is sha1_96.

prefer_stoc_hmac: Preferred HMAC algorithm from the server to the client. 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 the connection with the remote SFTP server and enter the SFTP client view.

Example

To connect to the SFTP server with IP address 10.1.1.2 using the default encryption algorithm, enter the following:

```
[SW4500]sftp 10.1.1.2
```

13 CONFIGURING PASSWORD CONTROL

This chapter describes how to use the following password control commands:

- display password-control
- display password-control blacklist
- display password-control super
- password
- password-control
- password-control enable
- password-control super
- reset password-control history-record
- reset password-control history-record super
- reset password-control blacklist

display password-control

Syntax

display password-control

View

Any view

Parameter

None

Description

Use the **display password-control** command to display the information about the global password control for all users.

Example

Display the information about the current global password control for all users.

```
[4500] display password-control
Global password settings for all users:
Password Aging:     Enabled (90 days)
Password Length:   Enabled (10 Characters)
Password History:   Enabled   (Max history-record  num : 6)
Password alert-before-expire :  7  days
Password  Authentication-timeout : 60 seconds
Password Attemp-failed action  :  Disable
Password History was last reset 38 days ago.
```

Table 48 describes the output fields of the display password-control command.

Table 48 Fields in Display Password- Control Command

Field	Description
Password Aging	Password aging time
Password Length	Minimum password length
Password History	History password recording
Password alert-before-expire	Alert time before password expiration
Password Authentication-timeout	Timeout for password authentication
Password Attemp-failed action	Password attempts limitation
History password was last reset 38 days ago	Time when the history password was last cleared

display password-control blacklist

Syntax

display password-control blacklist [username username | ipaddress ip-address]

View

Any view

Parameter

- *username*: Name of a user who has been added to the blacklist.
- *ip-address*: IP address of a user who has been added to the blacklist.

Description

Use the display password-control blacklist command to display the information about one or all users who have been added to the blacklist because of password attempt failure.

Example

Display the information about all the users who have been added to the blacklist because of password attempt failure.

```
[4500] display password-control blacklist
USERNAME                          IP
Jack                              10.1.1.2
The number of users in blacklist is :1
```

display password-control super

Syntax

display password-control super

View

Any view

Parameter

None

Description

Use the display password-control super command to display the information about the password control for super passwords, including the password aging time and the minimum password length.

Example

Display the information about the password control for super passwords.

```
<4500>display password-control super
 Super's password settings:
 Password Aging:                 Enabled(90 days)
 Password min-Length:            Enabled(10 Characters)
```

password

Syntax

password

View

Local user view

Parameter

None

Description

Use the password command to configure or change the system login password for a user.

Example

Configure the system login password for user test to 9876543210.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]local-user test
New local user added.
[4500-luser-test]password
Password:**********
confirm:**********
# Change the system login password for user test to 0123456789.
[4500-luser-test]password
Password:**********
Confirm :**********
Updating the password file ,please wait ...
```

password-control

Syntax

```
password-control aging aging-time
password-control length length
password-control login-attempt login-times [ exceed { lock | unlock
| locktime time } ]
password-control history max-record-num
password-control alert-before-expire alert-time
password-control authentication-timeout authentication-timeout
undo password-control { aging | length | login-attempt | exceed  |
history | alert-before-expire | authentication-timeout }
```

View

System view

Parameter

- *aging-time*: Password aging time. It ranges from 1 day to 365 days and defaults to 90 days.
- *length*: Minimum password length. It ranges from 4 characters to 32 characters and defaults to 10 characters.
- *login-times*: Login attempt times allowed for each user. It ranges from 2 to 10 and defaults to 3.
- *max-record-num*: Maximum number of history records allowed for each user. It ranges from 2 to 10 and defaults to 4.
- *alert-time*: Alert time. When the remaining usable time of a password is no more than this time, the user is alerted to the forthcoming password expiration. It ranges from 1 day to 30 days and defaults to 7 days.
- *authentication-timeout*: Timeout time for user authentication. It ranges from 30 seconds to 120 seconds and defaults to 60 seconds.
- *exceed*: Used to configure the procession mode used after login failures.
- *lock*: A procession mode. In this mode, a login-failure user is added to the blacklist and inhibited from re-login; only after the administrator manually remove this user from the blacklist, this user is allowed to log in the switch again.
- *locktime time*: A procession mode. In this mode, a login-failure user is inhibited from login in a certain time period, which ranges from 3 to 360 minutes and defaults to 120 minutes; only after this time passes, the user is allowed to log in the switch again.
- *unlock*: A procession mode. In this mode, a login-failure user is allowed to log in the switch again and again without any inhibition.

  By default, the system operates in locktime mode after a password authentication fails.

Description

Use the **password-control aging aging-time** command to configure an aging time for system login passwords.

Use the **password-control length length** command to configure the minimum password length for the system login passwords.

Use the **password-control login-attempt login-times** command to configure the maximum password attempt times allowed for each user.

Use the **password-control history max-record-num** command to configure the maximum number of history password records allowed for each user.

Use the **password-control alert-before-expire alert-time** command to configure the alert time, that is, the number of days when users are alerted ahead of their password expiration.

Use the **password-control authentication-timeout authentication-timeout** command to configure the timeout time for user password authentication.

Use the **password-control exceed** command to configure the procession mode used after password attempt failure.

Example

Configure the password aging time of the system login passwords to 100 days.

```
<4500>system-view
```

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

```
[4500] password-control aging 100
```

Configure the minimum password length of the system login passwords to eight characters.

```
[4500] password-control length 8
```

Configure the maximum password attempts times allowed for each user to five.

```
[4500] password-control login-attempt 5
```

Configure the maximum number of history password records allowed for each user to 10.

```
[4500] password-control history 10
```

Configure the alert time when users are alerted to their forthcoming expiration to seven days ahead of their expiration times.

```
[4500] password-control alert-before-expire  7
```

Configure the timeout time of the user password authentication to 100 seconds.

```
[4500] password-control authentication-timeout 100
```

Configure the maximum password attempt times to five, and configure the system to allow the attempt failure user to re-log in the switch 360 minutes after the failure.

```
[4500] password-control login-attempt 5 exceed locktime 360
```

password-control enable

Syntax

password-control { aging | **length** | **history } enable**
undo password-control { aging | **length** | **history } enable**

View

System view

Parameter

None

Description

Use the following password-control enable commands to enable the various password control functions of the system:

- Use the **password-control aging enable** command to enable password aging.
- Use the **password-control length enable** command to enable the limitation of the minimum password length.
- Use the **password-control history enable** command to enable the history password recording.

  When a password used to log in the switch expires, the switch requires the user to update the password, and automatically saves the history (old) password to a file in the flash memory. In this way, the switch can prevent any user from using one single password for a long time or an old password that was once used to enhance the security.
- Use the **undo password-control { aging | length | history } enable** command to disable password control.

  By default, password aging, limitation of minimum password length, and history password recording are all enabled.

  Related command: **password-control**.

Example

Enable password aging.

```
[4500]password-control aging  enable
Password aging enabled for all users. Default: 90 days.
```

Enable the limitation of the minimum password length.

```
[4500]password-control length  enable
Password minimum length enabled for all users. Default: 10
characters.
```

Disable password aging.

```
[4500]undo password-control aging
Password aging disabled for all users.
```

Enable history password recording.

```
[4500]password-control history enable
Password history enabled for all users.
```

Disable history password recording.

```
[4500]undo password-control history
Password history disabled for all users.
```

password-control super

Syntax

password-control super { aging aging-time | length min-length }
undo password-control super { aging | length }

View

System view

Parameter

- *aging-time*: Aging time for super passwords. It ranges from 1 day to 365 days and defaults to 90 days.
- *min-length*: Minimum length for super passwords. It ranges from 4 characters to 16 characters and defaults to 10 characters.

Description

Use the **password-control super** command to configure the parameters related with the supper passwords, including the password aging time and the minimum password length.

Use the **undo password-control super** command to restore the default settings for the super passwords.

The super passwords are used for the user who has logged in the switch and wants to change from a lower privilege level to a higher privilege level.

Example

Configure the aging time of the super passwords to 10 days.

```
<4500> system-view
System View: return to User View with Ctrl+Z.
[4500] password-control super aging 10
```

reset password-control history-record

Syntax

reset password-control history-record [username username]

View

User view

Parameter

username: Name of a user whose history password records will be deleted.

Description

Use the **reset password-control history-record** command to delete the history password records of all users.

Use the **reset password-control history-record username username** command to delete the history password records of a specific user.

Example

Delete the history password records of all users

```
<4500> reset password-control history-record
Are you sure to delete all  the  history record?[Y/N]
```

If you input "Y", the system deletes all the history password records of all users and gives the following prompt:

```
All historical passwords have been cleared for all users.
```

Delete the history password records of user test

```
<4500> reset password-control history-record username test
Are you sure to delete all the history record of user test ?[Y/N]
```

If you input "Y", the system deletes all the history password records of the specified user and gives the following prompt:

```
All historical passwords have been cleared for  user test.
```

reset password-control history-record super

Syntax

reset password-control history-record super [level level-value]

View

User view

Parameter

level-value: Privilege level, the history records of the super password for the users at this level will be deleted. This value ranges from 1 to 3.

Description

Use the **reset password-control history-record super level level-value** command to delete the history records of the super password for the users at the specified level.

Use the **reset password-control history-record super** command to delete the history records of all super passwords.

Example

Delete the history records of the super password for the users at level 2.

```
<4500>reset password-control history-record super level 2
Are you sure to clear  the  specified-level super password history
records?[Y/N]
```

If you input "Y", the system deletes the history records of the super password for the users at level 2.

reset password-control blacklist

Syntax

reset password-control blacklist [username username]

View

User view

Parameter

username username: Specifies a user name.

Description

Use the **reset password-control blacklist** command to delete all the user entries in the blacklist.

Use the **reset password-control blacklist username username** command to delete one specific user entry in the blacklist.

Example

Check the user information in the blacklist; as you can see, the blacklist contains three users: test, tes, and test2.

```
<4500>display password-control blacklist
USERNAME                        IP
test                            192.168.30.25
tes                             192.168.30.24
test2                           192.168.30.23
```

Delete user test from the blacklist

```
<4500> reset password-control blacklist user-name test
Are you sure to delete the  blacklist-users ?[Y/N]y
 All the blacklist users  have been cleared.
```

Check the current user information in the blacklist; as you can see, user test does not exist in the blacklist now.

```
[4500]display password-control blacklist
USERNAME                        IP
tes                             192.168.30.24
test2                           192.168.30.23
```

A BOOTROM INTERFACE

Accessing the Bootrom Interface

During the initial boot phase of the Switch the following prompt is displayed with a five second countdown timer allowing access to the bootrom:

```
Starting......

      ****************************************************
*
* SuperStack 4 Switch 4500 50-Port BOOTROM, Version 1.0
*
****************************************************

Copyright 2003-2005 3Com Corporation.  All Rights Reserved.
Creation date   : Jan 31 2005, 22:31:29
CPU type        : BCM4704
CPU Clock Speed : 200MHz
BUS Clock Speed : 33MHz
Memory Size     : 64MB
Mac Address     : 000fcbb77740


Press Ctrl-B to enter Boot Menu... 3
```

Before the countdown reaches 0, enter <CTRL>B

The timer is followed by a password prompt. The default is no password.

Press *Enter* to display the following boot menu:

```
          BOOT   MENU

1. Download application file to flash
2. Select application file to boot
3. Display all files in flash
4. Delete file from flash
5. Modify bootrom password
6. Enter bootrom upgrade menu
7. Skip current configuration file
8. Set bootrom password recovery
9. Set switch startup mode
0. Reboot

Enter your choice(0-9): 1
```

Boot Menu

The following section describes the various options available in the boot menu.

Download Application File to Flash

This option enables you to download all files into flash. Enter 1 at the prompt to display the following menu options:

```
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu
```

For further information on downloading see "Boot Menu File Download Commands" on page 459.

Select Application File to Boot

Select Option 2 at the prompt to display the following:

```
Select application file to boot
1. set application files
2. set configuration files
3. set web files
0. return

Enter your choice(0-3):
```

Enter Option 1 at the prompt to display the following:

```
             File
File Number  Size(bytes)     File Name
================================================
1(*)         4649088         s4h03_01_04s168.app

Free Space: 10491904 bytes

(*)-with main attribute;(b)-with backup attribute
(*b)-with both main and backup attribute

Please input the file number to be change:
```

An asterisk (*) indicates the current main boot file.

A similar screen will be displayed for the configuration files and the web files.

In each case, the file is given the attribute "main" or "backup".

Display all Files in Flash

Select Option 3 at the prompt to display the following:

```
             File
File Number  Size(bytes)     File Name
================================================
1            4               snmpboots
2            151             private-data.txt
3(*)         4649088         s4b03_01_04s168.app
4            576218          s4h03_04.web
5            10301           3comoscfg.def
6            10369           3comoscfg.cfg
7            10369           [test.cfg]

Free Space: 10460160 bytes
The current application file is s4b03_01_04s168.app
(*)-with main attribute;(b)-with backup attribute
(*b)-with both main and backup attribute
```

The current application file is name and an * indicates the file in the list.

If the filename is in brackets, for example `[test.cfg]`, this indicates that the file has been deleted from the CLI but is still present in the recycle-bin.

Delete File from Flash

Select Option 4 at the prompt to display the following:

```
             File
File Number  Size(bytes)     File Name
================================================
1            4               snmpboots
2            151             private-data.txt
3(*)         4649088         s4b03_01_04s168.app
```

```
              File
File Number   Size(bytes)     File Name
4             576218          s4h03_04.web
5             10301           3comoscfg.def
6             10369           3comoscfg.cfg
7             10369           [test.cfg]

Free Space: 10460160 bytes
The current application file is s4b03_01_04s168.app
(*)-with main attribute;(b)-with backup attribute
(*b)-with both main and backup attribute

Please input the file number to delete:
```

The current application file is name and an * indicates the file in the list.

If the filename is in brackets, for example `[test.cfg]`, this indicates that the file has been deleted from the CLI but is still present in the recycle-bin.

Modify Bootrom Password

Select Option 5 at the prompt to allow the bootrom access password to be changed as follows:

```
Old password:
New password: XXXX
Confirm password: XXXX

Current password has been changed successfully!
```

Enter Bootrom Upgrade Menu

Select Option 6 at the prompt to allow a bootrom file to be downloaded to Flash and then automatically upgrade the bootrom to the new version as follows:

```
Bootrom update menu:
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu
```

For further information on downloading see "Boot Menu File Download Commands" on page 459.

Skip Current Configuration File

Select Option 7 at the prompt to allow the Switch to be rebooted without loading the current configurations as follows:

```
The current setting is running configuration file when reboot.

Are you sure to skip current configuration file when reboot?
Yes or No(Y/N)
```

The Switch will reboot using the factory defaults.

Set Bootrom Password Recovery

Enter Option 8 at the prompt to allow the bootrom super password to be disabled or enabled. The following is displayed:

```
Warning: if disable the bootrom password recovery, the super
password based on switch mac address is invalid!

The current mode is enable bootrom password recovery.
```

```
Are you sure to disable bootrom password recovery? Yes or
No(Y/N) n
```

If the bootrom super password is disabled and the bootrom password (set at Boot Menu Option 5) is lost, bootrom access is no longer possible. If access to the bootrom menu is required, the Switch will need to be returned to 3Com for repair.

The super password is a fixed password that is based on the hardware of the Switch. Once the Switch has been registered with 3Com, this password can be supplied to the registered owner by contacting 3Com technical support.

Set Switch Startup Mode

Enter Option 9 at the prompt to allow the Power on Self Test (POST) mode to be selected. The following is displayed:

```
The current mode is fast startup mode!

Are you sure to change it to full startup mode? Yes or
No(Y/N)n
```

Full startup mode supplies additional POST information via the console.

Reboot

Enter Option 0 at the prompt to reboot the Switch. The following is displayed:

```
Starting......
```

Boot Menu File Download Commands

Enter Option 1 from the Boot menu to display the following download options:

Selecting a TFTP download

```
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu

Enter your choice(0-3): 1
Load File name           :s4b03_01_04s168.app
Switch IP address        :10.1.1.200
Server IP address        :10.1.1.177
Are you sure to download file to flash? Yes or No(Y/N)

Attached TCP/IP interface to netdrv0.
0x83fbb6a0 (tNetTask): arp info overwritten for a147a5b2 by
00:0d:54:9a:fa:20
Attaching network interface lo0...done.
Loading.................................................
..................
..............done
Free flash Space: 10491904 bytes
Writing
flash...................................................
...........
..done!

Please input the file attribute (main/backup/none):none
done!
```

Selecting a FTP download

```
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu

Enter your choice(0-3): 2
Load File name:s4b03_01_04s168.app
Switch IP address:10.1.1.200
Server IP address:10.1.1.177
FTP User Name            :anonymous
FTP User Password        :pass
Are you sure to download file to flash? Yes or No(Y/N) y
Loading.....done
Free flash Space: 10456064 bytes
Writing flash....done!
Please input the file attribute (main/backup/none):none
done!
```

Selecting an XModem download

```
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu

Enter your choice(0-3): 3
Please select your download baudrate:
1.  9600
2.* 19200
3.  38400
4.  57600
5.  115200
0.  Return

Enter your choice(0-5): 2
Download baudrate is 19200 bps
Please change the terminal's baudrate to 19200 bps and select
XMODEM protocol
Press enter key when ready

Now please start transfer file with XMODEM protocol
If you want to exit, Press <Ctrl+X>
Loading ...CCCCCCCCCCCCCCCCCCCCCCCCC

Please input the file attribute (main/backup/none):none
done!
```