1. Getting Started
2. Port
3. VLAN
4. Multicast
5. QoS/ACL
6. Integrated Management
7. STP
8. Security
10. System Management
11. Remote Power-feeding
12. Appendix

Quidway S3000-EI Series Ethernet Switches
Command Manual

VRP3.10
Quidway S3000-EI Series Ethernet Switches
Command Manual

Manual Version     T2-081929-20050625-C-1.04
Product Version    VRP3.10
BOM                31190229

Huawei Technologies Co., Ltd. provides customers with comprehensive technical support and service. If you purchase the products from the sales agent of Huawei Technologies Co., Ltd., please contact our sales agent. If you purchase the products from Huawei Technologies Co., Ltd. directly, Please feel free to contact our local office, customer care center or company headquarters.

Huawei Technologies Co., Ltd.

Address: Administration Building, Huawei Technologies Co., Ltd.,
Bantian, Longgang District, Shenzhen, P. R. China

Postal Code: 518129
Website: http://www.huawei.com
All Rights Reserved

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

Trademarks

HUAWEI, C&C08, EAST8000, HONET, ViewPoint, iNTess, ETS, DMC, TELLIN, InfoLink, Netkey, Quidway, SYNLOCK, Radium, M900/M1800, TELESIGHT, Quidview, Musa, Airbridge, Tellwin, Inmedia, VRP, DOPRA, iTELLIN, HUAWEI OptiX, C&C08iNET, NETENGINE, OptiX, iSite, U-SYS, iMUSE, OpenEye, Lansway, SmartAX, infoX, and TopEng are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this manual are the property of their respective holders.

Notice

The information in this manual is subject to change without notice. Every effort has been made in the preparation of this manual to ensure accuracy of the contents, but all statements, information, and recommendations in this manual do not constitute the warranty of any kind, express or implied.
About This Manual

Release Notes

The product version that corresponds to the manual is VRP3.10.

Related Manuals

The following manuals provide more information about the Quidway S3000-EI Series Ethernet Switches.

<table>
<thead>
<tr>
<th>Manual</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quidway S3026C-PWR Ethernet Switch Installation Manual</td>
<td>Introduces the system installation, booting, configuration and maintenance of S3026C-PWR Ethernet Switch.</td>
</tr>
<tr>
<td>Quidway S3000-EI Series Ethernet Switches Installation Manual</td>
<td>Introduces the system installation, booting, configuration and maintenance of S3000-EI Series Ethernet Switches.</td>
</tr>
<tr>
<td>Quidway S3000-EI Series Ethernet Switches Operation Manual</td>
<td>Introduces such modules as getting started, port, VLAN, multicast, QoS/ACL, integrated management, STP, security, network protocols, remote power-feeding, and system management.</td>
</tr>
</tbody>
</table>

Organization

*Quidway S3000-EI Series Ethernet Switches Command Manual* consists of the following parts:

- **Getting Started**
  This module introduces the commands used for accessing the Ethernet Switch.

- **Port**
  This module introduces the commands used for configuring Ethernet port, link aggregation and port isolation.

- **VLAN**
  This module introduces the commands used for configuring VLAN.

- **Multicast**
This module introduces the commands used for configuring multicast protocols.

- **QoS/ACL**
  This module introduces the commands used for configuring QoS/ACL.

- **Integrated Management**
  This module introduces the commands used for integrated management.

- **STP**
  This module introduces the commands used for configuring STP.

- **Security**
  This module introduces the commands used for configuring 802.1X, AAA & RADIUS, and HABP.

- **Network Protocol**
  This module introduces the commands used for configuring network protocol, including ARP, DHCP snooping, and IP performance.

- **System Management**
  This module introduces the commands used for system management and maintenance.

- **Remote Power-feeding**
  This module introduces remote power-feeding configuration.

- **Appendix**
  This appendix lists all the commands that appear in the manuals.

**Intended Audience**

The manual is intended for the following readers:

- Network engineers
- Network administrators
- Customers who are familiar with network fundamentals

**Conventions**

The manual uses the following conventions:
I. General conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arial</td>
<td>Normal paragraphs are in Arial.</td>
</tr>
<tr>
<td><strong>Boldface</strong></td>
<td>Headings are in <strong>Boldface</strong>.</td>
</tr>
<tr>
<td>Courier New</td>
<td>Terminal Display is in Courier New.</td>
</tr>
</tbody>
</table>

II. Command conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Boldface</strong></td>
<td>The keywords of a command line are in <strong>Boldface</strong>.</td>
</tr>
<tr>
<td><em>italic</em></td>
<td>Command arguments are in <em>italic</em>.</td>
</tr>
<tr>
<td>[]</td>
<td>Items (keywords or arguments) in square brackets [] are optional.</td>
</tr>
<tr>
<td>{x</td>
<td>y</td>
</tr>
<tr>
<td>[x</td>
<td>y</td>
</tr>
<tr>
<td>{x</td>
<td>y</td>
</tr>
<tr>
<td>[x</td>
<td>y</td>
</tr>
<tr>
<td>#</td>
<td>A line starting with the # sign is comments.</td>
</tr>
</tbody>
</table>

III. GUI conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;&gt;</td>
<td>Button names are inside angle brackets. For example, click the &lt;OK&gt; button.</td>
</tr>
<tr>
<td>[]</td>
<td>Window names, menu items, data table and field names are inside square brackets. For example, pop up the [New User] window.</td>
</tr>
<tr>
<td>/</td>
<td>Multi-level menus are separated by forward slashes. For example, [File/Create/Folder].</td>
</tr>
</tbody>
</table>
IV. Keyboard operation

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Key&gt;</td>
<td>Press the key with the key name inside angle brackets. For example, &lt;Enter&gt;, &lt;Tab&gt;, &lt;Backspace&gt;, or &lt;A&gt;.</td>
</tr>
<tr>
<td>&lt;Key1+Key2&gt;</td>
<td>Press the keys concurrently. For example, &lt;Ctrl+Alt+A&gt; means the three keys should be pressed concurrently.</td>
</tr>
<tr>
<td>&lt;Key1, Key2&gt;</td>
<td>Press the keys in turn. For example, &lt;Alt, A&gt; means the two keys should be pressed in turn.</td>
</tr>
</tbody>
</table>

V. Mouse operation

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select</td>
<td>Press and hold the primary mouse button (left mouse button by default).</td>
</tr>
<tr>
<td>Click</td>
<td>Select and release the primary mouse button without moving the pointer.</td>
</tr>
<tr>
<td>Double-Click</td>
<td>Press the primary mouse button twice continuously and quickly without moving the pointer.</td>
</tr>
<tr>
<td>Drag</td>
<td>Press and hold the primary mouse button and move the pointer to a certain position.</td>
</tr>
</tbody>
</table>

VI. Symbols

Eye-catching symbols are also used in the manual to highlight the points worthy of special attention during the operation. They are defined as follows:

⚠️ **Caution, Warning:** Means reader be extremely careful during the operation.

‼️ **Note:** Means a complementary description.
# Table of Contents

## Chapter 1 Logging in Switch Commands ................................................................. 1-1
1.1 Logging in Switch Commands .............................................................................. 1-1
  1.1.1 authentication-mode ....................................................................................... 1-1
  1.1.2 auto-execute command .................................................................................. 1-2
  1.1.3 command-privilege level ................................................................................. 1-3
  1.1.4 databits .......................................................................................................... 1-4
  1.1.5 display history-command ............................................................................... 1-4
  1.1.6 display user-interface .................................................................................... 1-5
  1.1.7 display users .................................................................................................. 1-6
  1.1.8 flow-control .................................................................................................. 1-7
  1.1.9 free user-interface .......................................................................................... 1-7
  1.1.10 header .......................................................................................................... 1-8
  1.1.11 history-command max-size .......................................................................... 1-10
  1.1.12 idle-timeout .................................................................................................. 1-10
  1.1.13 language-mode ............................................................................................ 1-11
  1.1.14 lock .............................................................................................................. 1-12
  1.1.15 parity .......................................................................................................... 1-12
  1.1.16 protocol inbound ......................................................................................... 1-13
  1.1.17 quit ............................................................................................................... 1-13
  1.1.18 return .......................................................................................................... 1-14
  1.1.19 screen-length .............................................................................................. 1-14
  1.1.20 send ............................................................................................................ 1-15
  1.1.21 service-type ................................................................................................. 1-16
  1.1.22 set authentication password ....................................................................... 1-17
  1.1.23 shell ............................................................................................................ 1-18
  1.1.24 speed ......................................................................................................... 1-19
  1.1.25 stopbits ...................................................................................................... 1-19
  1.1.26 super ......................................................................................................... 1-20
  1.1.27 super password ......................................................................................... 1-21
  1.1.28 sysname ..................................................................................................... 1-22
  1.1.29 system-view .............................................................................................. 1-22
  1.1.30 telnet .......................................................................................................... 1-23
  1.1.31 user-interface ............................................................................................ 1-23
  1.1.32 user privilege level ..................................................................................... 1-24

## Chapter 2 System IP Configuration Commands ...................................................... 2-1
2.1 System IP Configuration Commands .................................................................... 2-1
  2.1.1 description ..................................................................................................... 2-1
Chapter 1 Logging in Switch Commands

1.1 Logging in Switch Commands

1.1.1 authentication-mode

Syntax

authentication-mode { password | scheme | none }

View

User interface view

Parameter

password: Perform local password authentication.
scheme: Perform local or remote authentication of username and password.
none: Perform no authentication.

Description

Using authentication-mode command, you can configure the authentication method for login user.

This command with the password parameter indicates to perform local password authentication, that is, you need to configure a login password using the set authentication password { cipher | simple } password command.

This command with the scheme parameter indicates to perform authentication of local or remote username and password. The type of the authentication depends on your configuration. For detailed information, see “Security” section.

By default, users logging in via the Console port do not need to pass any terminal authentication, whereas the password is required for authenticating the Modem and Telnet users when they log in.

Example

# Configure local password authentication.
[Quidway-ui-aux0] authentication-mode password
1.1.2 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

Using auto-execute command command, you can configure to automatically run a specified command. When a user logs in, the command configured will be executed automatically. Using undo auto-execute command command, you can configure not to run the command automatically.

This command is usually used to configure the telnet command on the terminal, which will connect the user to a designated device automatically.

By default, auto run is disabled.

Caution:

- If you execute this command, the user-interface can no longer be used to perform routine configurations on the local system. Therefore use caution when using this command.
- Ensure that you will be able to log into the system in some other way to cancel the configuration, before you configure the auto-execute command command and save the configuration.

Example

# Configure to automatically telnet 10.110.100.1 after the user logs in via VTY 0.

[Quidway-ui-vty0] auto-execute command telnet 10.110.100.1
1.1.3 command-privilege level

Syntax

command-privilege level level view view command
undo command-privilege view view command

View

System view

Parameter

level: Specifies the command level, ranging from 0 to 3.

view: Specifies the command view, which can be any of the views supported by the switch.

command: Specifies the command to be configured.

Description

Using command-privilege level command, you can configure the priority of the specifically command of the specifically view. Using undo command-privilege view command, you can restore the default command priority.

The command levels include visit, monitoring, system, and management, which are identified as 0 through 3 respectively. The network administrator can customize the command levels as needed.

When users log into the switch, the commands they can use depend jointly on the user level settings and the command level settings on the user interface. If the two types of settings differ,

- For the users using AAA/RADIUS authentication, the commands they can use are determined by the user level settings. For example, if a use is set to level 3 and the command level on the VTY 0 user interface is level 1, he or she can only use the commands of level 3 or lower when logging into the switch from the VTY 0 user interface.
- For the users using RSA public key authentication, the commands they can use are determined by the command level settings on the user interface.

By default, ping, tracert, and telnet are at visit level (0); display and debugging are at monitoring level (1); all configuration commands are at system level (2); and FTP, XMODEM, TFTP and commands for file system operations are at management level (3).

Example

# Configure the precedence of the command "interface" as 0.
[Quidway] command-privilege level 0 view system interface
1.1.4 databits

Syntax

databits { 7 | 8 }
undo databits

View

User interface view

Parameter

7: The data bits are 7.
8: The data bits are 8.

Description

Using **databits** command, you can configure the data bits for AUX (Console) port. Using **undo databits** command, you can restore the default bits of the AUX (Console).

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

By default, the value is 8.

Example

# Configure the data bits of AUX (Console) port to 7 bits.

    [Quidway-ui-aux0] databits 7

1.1.5 display history-command

Syntax

display history-command

View

Any view

Parameter

None

Description

Using **display history-command** command, you can view the saved history commands.

For the related command, see **history-command max-size**.
Example

# Display history commands.
<Quidway> display history-command
sys
quit
display his

1.1.6 display user-interface

Syntax

display user-interface [ type number ] [ number ]

View

Any view

Parameter

type: Specifies the type of a user interface.
number: Specifies the number of a user interface.

Description

Using display user-interface command, you can view the relational information of the user interface. The displayed information includes user interface type, absolute/relative index, transmission speed, priority, and authentication methods.

Example

# Display the relational information of user interface 0.
<Quidway> display user-interface 0
Idx  Type   Tx/Rx  Modem Privi  Auth
F 0  AUX 0  9600           3   N

+: Current user-interface is active.
F: Current user-interface is active and work in async mode.
Idx: Absolute index of user-interface.
Type: Type and relative index of user-interface.
Privi: The privilege of user-interface.
Auth: The authentication mode of user-interface.
A: Authenticate use AAA.
N: Current user-interface need not authentication.
P: Authenticate use current UI’s password.
Table 1-1 Output description of the **display user-interface** command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>Current user interface is in use</td>
</tr>
<tr>
<td>F</td>
<td>Current user interface is in use and work in asynchronous mode</td>
</tr>
<tr>
<td>Idx</td>
<td>Absolute index of user interface</td>
</tr>
<tr>
<td>Type</td>
<td>Type and relative index of user interface</td>
</tr>
<tr>
<td>Tx/Rx</td>
<td>User interface speed</td>
</tr>
<tr>
<td>Modem</td>
<td>Modem operation mode</td>
</tr>
<tr>
<td>Privi</td>
<td>Which levels of commands can be used after logging in from the user interface</td>
</tr>
<tr>
<td>Auth</td>
<td>User interface authentication method</td>
</tr>
</tbody>
</table>

1.1.7 **display users**

**Syntax**

```plaintext
display users [ all ]
```

**View**

Any view

**Parameter**

all: Display the information of all user interfaces.

**Description**

Using **display users** command, you can view the information of the user interface.

**Example**

```plaintext
# Display the information of the current user interface.
[Quidway] display users

UI   Delay Type Ipaddress Username
F    0   AUX 0 00:00:00
```

Table 1-2 Output description of the **display users** command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>Current user interface is in use and work in asynchronous mode.</td>
</tr>
<tr>
<td>UI</td>
<td>Number of the first list is the absolute number of user interface. Number of the second list is the relative number of user interface.</td>
</tr>
</tbody>
</table>
### 1.1.8 flow-control

**Syntax**

```plaintext
flow-control { hardware | none | software }
undo flow-control
```

**View**

User interface view

**Parameter**

- **hardware**: Configures to perform hardware flow control.
- **none**: Configures no flow control.
- **software**: Configures to perform software flow control.

**Description**

Using `flow-control` command, you can configure the flow control mode on AUX (Console) port. Using `undo flow-control` command, you can restore the default flow control mode.

By default, the value is **none**. That is, no flow control will be performed.

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

**Example**

```plaintext
# Configure software flow control on AUX (Console) port.
[Quidway-ui-aux0] flow-control software
```

### 1.1.9 free user-interface

**Syntax**

```plaintext
free user-interface [ type ] number
```

**View**

User view
Parameter

*type*: Specifies the user interface type.

*num*: Specifies the absolute/relative number of the user interface. Configured together with the *type*, it will specify the user interface number of the corresponding type. If the *type* is not specified, *num* will specify an absolute user interface number.

Description

Using **free user-interface** command, you can reset a specified user interface. The user interface will be disconnected after the command is executed. Note that the current user interface cannot be cleared.

Example

```bash
# Reset user interface 1 after logged in to the switch via user interface 0.
<Quidway> free user-interface 1
Are you sure to free user-interface vty0
 [Y/N] 
```

After the command is executed, user interface 1 will be disconnected. It will not be connected to the switch until you log in via the user interface 1 for the next time.

1.1.10 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.

*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 modes: one is to input all the text in one line, and altogether 256 characters can be input; the other is to input all the text in several lines using the <Enter> key. The text
starts and ends with the first character. After inputting the end character, press the <Enter> key to exit the interact process.

Description

Using header command, you can configure to display header when user login. Using undo header command, you can configure not to display the header.

When the users log in the switch, if a connection is activated, the login header will be displayed. After the user successfully logs in the switch, the shell header will be displayed.

Note that 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

[Quidway] 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.

[Quidway] quit
<Quidway> quit
Please press ENTER
SHELL: Hello! Welcome (The initial character "%" is not the header contents)
<Quidway>

Mode 2: Input in several lines

[Quidway] 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)
[Quidway]

When you log on the switch again, the terminal displays the configured session establishment title.
[Quidway] quit
<Quidway> quit
Please press ENTER
%SHELL: (The initial character "%" is the header contents)
Hello! Welcome
<Quidway>

1.1.11 history-command max-size

Syntax

history-command max-size value
undo history-command max-size

View

User interface view

Parameter

value: Defines the size of the history buffer, ranging from 0 to 256. By default, the size is 10, that is, 10 history commands can be saved.

Description

Using history-command max-size command, you can configure the size of the history command buffer. Using undo history-command max-size command, you can restore default size of the history command buffer.

Example

# Set the history buffer to 20, namely saving 20 history commands.
[Quidway-ui-aux0] history-command max-size 20

1.1.12 idle-timeout

Syntax

idle-timeout minutes [ seconds ]
undo idle-timeout

View

User interface view
Parameter

- **minutes**: Specifies the minute, ranging from 0 to 35791.
- **seconds**: Specifies the second, ranging from 0 to 59.

Description

Using the `idle-timeout` command, you can configure the timeout function. If there is no user operation performed before idle-timeout expires, the user interface will be disconnected. Using the `undo idle-timeout` command, you can restore the default idle-timeout.

`idle-timeout 0` means disabling idle-timeout.

By default, idle-timeout is set to 10 minutes.

Example

```
# Configure the timeout value to 1 minute on the AUX user interface.
[Quidway-ui-aux0] idle-timeout 1 0
```

1.1.13 **language-mode**

Syntax

```
language-mode { chinese | english }
```

View

User view

Parameter

- **chinese**: Configures the language environment of command line interface as Chinese.
- **english**: Configures the language environment of command line interface as English.

Description

Using the `language-mode` command, you can switch between different language environments of command line interface for convenience of different users.

By default, the value is English.

Example

```
# Switch from English mode to Chinese mode.
<Quidway> language-mode chinese
```
1.1.14  lock

Syntax

lock

View

User view

Parameter

None

Description

Using lock command, you can lock the user interface to prevent unauthorized user from operating it.

Example

# Lock the current user interface.
<Quidway> lock
Password: xxxx
Again: xxxx

1.1.15  parity

Syntax

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

View

User interface view

Parameter

even: Configures to perform even parity.
mark: Configures to perform mark parity.
none: Configures not to perform parity.
odd: Configures to perform odd parity.
space: Configures to perform space parity.

Description

Using parity command, you can configure the parity mode on AUX (Console) port. Using undo parity command, you can restore the default parity mode.
This command can only be performed in AUX user interface view.
By default, the mode is set to none.

Example

```
# Set mark parity on the AUX (Console) port.
[Quidway-ui-aux0] parity mark
```

1.1.16 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

Using the `protocol inbound` command, you can configure the protocols supported by a designated user interface.

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

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

Example

```
# Configure SSH protocol supported by VTY0 user interface.
[Quidway-ui-vty0] protocol inbound ssh
```

1.1.17 quit

Syntax

```
quit
```

View

Any view

Parameter

None
Description

Using `quit` command, you can return to the lower level view from the current view. If the current view is user view, you can quit the system.

There are three levels of views, which are listed from low to high as follows:
- User view
- System view
- VLAN view, Ethernet port view, and so on.

For the related commands, see `return, system-view`.

Example

# Return to user view from system view.
[Quidway] quit
<Quidway>

1.1.18 return

Syntax

`return`

View

System view

Parameter

None

Description

Using `return` command, you can return to user view from a view other than user view. Combination key `<Ctrl+Z>` performs the same function with the `return` command.

For the related command, see `quit`.

Example

# Return to user view from system view.
[Quidway] return
<Quidway>

1.1.19 screen-length

Syntax

`screen-length screen-length`

`undo screen-length`
View

User interface view

Parameter

*screen-length*: Specifies how many lines can be displayed on a screen, ranging from 0 to 512. The default value is 24.

Description

Using *screen-length* command, you can configure how many lines that can be displayed on a screen of the terminal. Using *undo screen-length* command, you can restore the default number of terminal information lines displayed on the terminal screen.

The *screen-length 0* command is used to disable this function.

Example

```
# Configure the lines that can be displayed on a screen as 20 lines.
[Quidway-ui-aux0] screen-length 20
```

1.1.20 send

Syntax

```
send { all | number | type number }
```

View

User view

Parameter

*all*: Configures to send message to all user interfaces.

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

*number*: Specifies the absolute/relative number of the user interface.

Description

Using *send* command, you can send messages between different user interfaces.

Example

```
# Send message to all the user interfaces.
<Quidway> send all
```
1.1.21 service-type

Syntax

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

View

Local-user view

Parameter

- **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**: Specifies user type as SSH.
- **telnet**: Specifies user type as Telnet.
- **level level**: Specifies the level of Telnet or SSH users. The argument level is an integer in the range of 0 to 3 and defaults to 1.

Description

Using **service-type** command, you can configure which level of command a user can use after logon. Using **undo service-type** command, you can restore the default level of command a user can use after logon.

Commands are classified into four levels, namely visit level, monitoring level, system level and management level. They are introduced as follows:

- **Visit level**: Commands of this level involve command of network diagnosis tool (such as **ping** and **tracert**), command of switch between different language environments of user interface (**language-mode**), and **telnet** command etc. The operation of saving configuration file is not allowed on this level of commands.
- **Monitoring level**: Commands of this level, including the **display** command and the **debugging** command, are used for system maintenance, service fault diagnosis, etc. The operation of saving the configuration file is not allowed on this level of commands.
- **System level**: Service configuration commands, including routing command and commands on each network layer, are used to provide direct network service to the user.
Management level: These are commands that influence the basic operation of the system and system support module, which plays a supporting role on service. Commands of this level involve file system commands, FTP commands, TFTP commands, XModem downloading commands, user management commands, and level setting commands.

Example

```
# Configure the user zbr to use commands at level 0 after logon.
[Quidway] local-user zbr
[Quidway-luser-zbr] service-type telnet level 0

# Quit the system and logs on with username “zbr” again. Now only the commands at level 0 are listed on the terminal.
[Quidway] quit
<Quidway> ?
```

User view commands:
- language-mode Specify the language environment
- ping Ping function
- quit Exit from current command view
- super Privilege specified user priority level
- telnet Establish one TELNET connection
- tracert Trace route function

1.1.22 set authentication password

Syntax

```
set authentication password { cipher | simple } password
undo set authentication password
```

View

User interface view

Parameter

- **cipher**: Configure encrypted text password.
- **simple**: Configure plain text password.
- **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. The result is determined by the input. A plain text password is a sequential character string of no more than 16 digits, for example, huawei918. The length of an encrypted password must be 24 digits and in encrypted text, for example, \_(_[TT8F]Y\sSQ=\^Q\'MAF4<1!!.

Huawei Technologies Proprietary
Description

Using `set authentication password` command, you can configure the password for local authentication. Using `undo set authentication password` command, you can cancel local authentication password.

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

⚠️ Note:

By default, password is required to be set for authenticating the users connecting via Modem or Telnet. If no password has been set, the following prompt will be displayed “Login password has not been set!”

Example

# Configure the local authentication password on VTY 0 to huawei.

```
[Quidway-ui-vty0] set authentication password simple huawei
```

1.1.23 shell

Syntax

```
shell
undo shell
```

View

User interface view

Parameter

None

Description

Using `shell` command, you can enable terminal service of a user interface. Using `undo shell` command, you can disable the terminal service of a user interface.

By default, terminal service is enabled.

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

- For the sake of security, the `undo shell` command can only be used on the user interfaces other than the AUX user interface.
- You cannot use this command on the user interface via which you log in.
You will be asked to confirm before executing this command on any legal user interface.

Example

# Disable terminal service on the vty user interface 0 to 4 after logging in to the switch via user interface 0.
[Quidway] user-interface vty 0 4
[Quidway-ui-vty0-4] undo shell

# The following message will be displayed on the Telnet terminal after logon.
Connection to host lost.

1.1.24  speed

Syntax

speed speed-value
undo speed

View

User interface view

Parameter

speed-value: Specifies the transmission rate on the AUX (Console) port in bit/s, which can be 300, 600, 1200, 4800, 9600, 19200, 38400, 57600, 115200 or 409600. The default rate is 9600bit/s.

Description

Using speed command, you can configure the transmission rate on the AUX (Console) port. Using undo speed command, you can restore the default rate.

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

Example

# Configure the transmission speed on the AUX (Console) port as 9600bit/s.
[Quidway-ui-aux0] speed 9600

1.1.25  stopbits

Syntax

stopbits { 1 | 1.5 | 2 }
undo stopbits
View

User interface view

Parameter

1: Sets 1 stop bit.
1.5: Sets 1.5 stop bits.
2: Sets 2 stop bits.

Description

Using `stopbits` command, you can configure the stop bits on the AUX (Console) port. Using `undo stopbits` command, you can restore the default stop bits.

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

By default, the value is 1.

Example

```
# Configure 2 stop bits on the AUX (Console) port.
[Quidway-ui-aux0] stopbits 2
```

1.1.26 super

Syntax

```
super [ level ]
```

View

User view

Parameter

`level`: User level, ranging 0 to 3. The default value is 3.

Description

Using `super` command, you can enable the user to change to user level from the current user level. If the user has set the `super password [ level level ] { simple | cipher } password`, then user password of the higher level is needed, or the former user level will not change.

Login users are classified into four levels that correspond to the four command levels respectively. After users of different levels log in, they can only use commands at the levels that are equal to or lower than its own level.

For the related commands, see `super password`, `quit`. 
Example

```bash
# change to user level 3 from the current user level.
<Quidway> super 3
Password:
```

1.1.27 super password

**Syntax**

```
super password [ level level ] { simple | cipher } password
undo super password [ level level ]
```

**View**

System view

**Parameter**

`level`: User level, ranging from 1 to 3. The default value is 3, i.e. do not specify user level. It means the password to be set is used for entering level 3.

`simple`: Configure to display the password in plain text.

`cipher`: Configure to display the password in encrypted 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 either be in encrypted text or in plain text. The result is determined by the input. A plain text password is a sequential character string of no more than 16 digits, for example, huawei918. The length of an encrypted password must be 24 digits and in encrypted text, for example, `_(TT8F]Y\55Q=^Q`MAF4<1!!.

**Description**

Using `super password` command, you can configure the password for changing the user from a lower level to a higher level. In order 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. Only when correct password is input for three times, can the user switch to the higher level. Otherwise, the original user level will remain unchanged. Using `undo super password` command, you can cancel the current settings.

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

**Example**

```bash
# Configure the password to zbr for changing the user from the current level to level 3.
```
1.1.28 sysname

Syntax

sysname text
undo sysname

View

System view

Parameter

text: Specifies the hostname with a character string, ranging from 1 to 30 characters. The default name is Quidway.

Description

Using sysname command, you can configure the hostname of the switch. Using undo sysname command, you can restore the default hostname.

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

Example

# Configure the hostname of switch to Switch.

[Quidway] sysname Switch

[Switch]

1.1.29 system-view

Syntax

system-view

View

User view

Parameter

None

Description

Using system-view command, you can enter system view from user view. For the related commands, see quit, return.
Command Manual - Getting Started
Quidway S3000-EI Series Ethernet Switches

Chapter 1  Logging in Switch Commands

Example

# Enter system view from user view.
<Quidway> system-view
 [Quidway]

1.1.30  telnet

Syntax

telnet { hostname | ip-address } [ service-port ]

View

User view

Parameter

hostname: Specifies the host name of the remote switch. It is configured using the ip host command.

ip-address: Specifies the IP address of the remote switch.

service-port: Designates the TCP port on the remote switch providing Telnet service, ranging from 0 to 65535.

Description

Using telnet command, you can log in to another switch from the current one via telnet for remote management. To terminate the Telnet logon, press <Ctrl+K>

By default, when the service-port is not specified, the default telnet port number is 23.

For the related command, see display tcp status.

Example

# Log in to switch Quidway2 at 129.102.0.1 from the current Quidway1 switch.
<Quidway1> telnet 129.102.0.1
<Quidway2>

1.1.31  user-interface

Syntax

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

View

System view
Parameter

- **type**: Specifies 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

```
# Enter user interface view 0 through 5, that is, 1 AUX (Console) port user interface view and 5 VTY user interface views.
[Quidway] user-interface 0 5
[Quidway-ui0-5]
```

1.1.32 user privilege level

Syntax

```
user privilege level level
undo user privilege level
```

View

User interface view

Parameter

- **level**: Specifies which level of command a user can use after logon from the specifically user interface, ranging from 0 to 3.

Description

Using `user privilege level` command, you can configure which level of command a user can use after logon from the specifically user interface, so that a user can use all the available commands at this level. Using `undo user privilege level` command, you can restore the default level of command a user can use after logon from the specifically user interface.

By default, a user can access the commands at Level 3 after logging in through the AUX user interface, and the commands at Level 0 after logging in through the VTY user interface.

Example

```
# Configure to use commands level 0 after logging in from VTY 0 user interface.
```
[Quidway-ui-vty0] user privilege level 0

# After you telnet from VTY 0 user interface to the switch, you will view the terminal only displays commands at level 0.

<Quidway> ?

User view commands:

language-mode Specify the language environment
ping Ping function
quit Exit from current command view
super Privilege specified user priority level
telnet Establish one TELNET connection
tracert Trace route function
Chapter 2  System IP Configuration Commands

2.1  System IP Configuration Commands

2.1.1  description

Syntax

```
description string
undo description
```

View

VLAN interface view

Parameter

```
string: Description character string of management VLAN interface, ranges from 1 to 80 characters. The default character string is HUAWEI, Quidway Series, Vlan-interface Interface. Vlan-interface1 is the management VLAN interface name.
```

Description

Using `description` command, you can configure the description character string of management VLAN interface. Using `undo description` command, you can restore the default description character string of management VLAN interface.

For the related command, see `display interface vlan-interface`.

Example

```
# Configure the description character string of management VLAN interface as RESEARCH.
[Quidway-Vlan-interface1] description RESEARCH
```

2.1.2  display interface vlan-interface

Syntax

```
display interface vlan-interface [vlan_id]
```

View

Any view
Parameter

\textit{vlan\_id}: ID of management VLAN interface, ranging from 1 to 4094.

Description

Using \texttt{display interface vlan-interface} command, you can view the related information about management VLAN interface such as physical status and link status of management VLAN interface, Ethernet frame format, MAC address, IP address and sub-net mask, description character string and MTU, etc.

For the related command, see \texttt{interface vlan-interface}.

Example

# Display related information about management VLAN interface.

```bash
<Quidway> display interface vlan-interface 1
Vlan-interface1 current state : DOWN
Line protocol current state : DOWN
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc07-4101
Internet Address is 10.1.1.1/24 Primary
Description : HUAWEI, Quidway Series, Vlan-interface1 Interface
The Maximum Transmit Unit is 1500
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan-interface1 current state</td>
<td>The current state of management VLAN interface</td>
</tr>
<tr>
<td>Line protocol current state</td>
<td>The current state of Line protocol</td>
</tr>
<tr>
<td>IP Sending Frames’ Format</td>
<td>Ethernet frame format</td>
</tr>
<tr>
<td>Hardware address</td>
<td>MAC address corresponding management VLAN interface</td>
</tr>
<tr>
<td>Internet Address</td>
<td>IP address</td>
</tr>
<tr>
<td>Description</td>
<td>management VLAN interface description character string</td>
</tr>
<tr>
<td>The Maximum Transmit Unit</td>
<td>The Maximum Transmit Unit</td>
</tr>
</tbody>
</table>

Table 2-1 Output description of display interface vlan-interface command

2.1.3 \texttt{display ip host}

Syntax

\texttt{display ip host}
View

Any view

Parameter

None

Description

Using **display ip host** command, you can view all the host names and their IP addresses.

Example

```
# Display all the host names and their IP addresses.
<Quidway> display ip host

<table>
<thead>
<tr>
<th>Host</th>
<th>Age</th>
<th>Flags</th>
<th>Address(es)</th>
</tr>
</thead>
<tbody>
<tr>
<td>My</td>
<td>0</td>
<td>static</td>
<td>1.1.1.1</td>
</tr>
<tr>
<td>Aa</td>
<td>0</td>
<td>static</td>
<td>2.2.2.4</td>
</tr>
</tbody>
</table>
```

**Table 2-2** Output description of **display ip host** command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Host name</td>
</tr>
<tr>
<td>Age</td>
<td>term of validity</td>
</tr>
<tr>
<td>Flags</td>
<td>Flags</td>
</tr>
<tr>
<td>Address(es)</td>
<td>IP address of the host</td>
</tr>
</tbody>
</table>

**2.1.4 display ip interface vlan-interface**

Syntax

```
display ip interface vlan-interface vlan-id
```

View

Any view

Parameter

```
vlan-id: Specifies the management VLAN interface ID.
```

Description

Using **display ip interface vlan-interface** command, you can view the information about the management VLAN interface.
Example

# Display the information about the management VLAN interface 1.
<Quidway> display ip interface vlan-interface 1
Vlan-interface1 current state : DOWN ,
Line protocol current state : DOWN
Internet Address is 1.1.1.1/8 Primary
Broadcast address : 1.255.255.255
The Maximum Transmit Unit : 1500 bytes
input packets : 0, bytes : 0, multicasts : 0
output packets : 0, bytes : 0, multicasts : 0

Table 2-3 Output description of display ip interface vlan-interface command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan-interface1 current state</td>
<td>The current state of management VLAN interface</td>
</tr>
<tr>
<td>Line protocol current state</td>
<td>The current state of Line protocol</td>
</tr>
<tr>
<td>Internet Address</td>
<td>IP address</td>
</tr>
<tr>
<td>Broadcast address</td>
<td>Broadcast address</td>
</tr>
<tr>
<td>The Maximum Transmit Unit</td>
<td>The Maximum Transmit Unit</td>
</tr>
</tbody>
</table>

2.1.5 display ip routing-table

Syntax

display ip routing-table

View

Any view

Parameter

None

Description

Using **display ip routing-table** command, you can view the routing table summary. This command displays routing table information in summary form. Each line represents one route. The contents include destination address/mask length, protocol, preference, metric, next hop and output interface.

Only current used route, i.e., best route, is displayed using **display ip routing-table** command.
Example

# View the summary of routing table.
<Quidway> display ip routing-table
Routing Table: public net

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Protocol</th>
<th>Pre</th>
<th>Cost</th>
<th>Nexthop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.0/24</td>
<td>DIRECT</td>
<td>0</td>
<td>0</td>
<td>1.1.1.1</td>
<td>Vlan-interface1</td>
</tr>
<tr>
<td>1.1.1.1/32</td>
<td>DIRECT</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoopBack0</td>
</tr>
<tr>
<td>127.0.0.0/8</td>
<td>DIRECT</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoopBack0</td>
</tr>
<tr>
<td>127.0.0.1/32</td>
<td>DIRECT</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoopBack0</td>
</tr>
</tbody>
</table>

Table 2-4 Description of information generated by the command display ip routing-table

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination/Mask</td>
<td>Destination address/Mask length</td>
</tr>
<tr>
<td>Protocol</td>
<td>Routing protocol</td>
</tr>
<tr>
<td>Pre</td>
<td>Routing preference</td>
</tr>
<tr>
<td>Cost</td>
<td>Cost</td>
</tr>
<tr>
<td>Nexthop</td>
<td>Next hop address</td>
</tr>
<tr>
<td>Interface</td>
<td>Output interface, through which the data packet destined for the destination network segment is sent</td>
</tr>
</tbody>
</table>

2.1.6 display ip routing-table acl

Syntax

display ip routing-table acl { acl-number | acl-name } [ verbose ]

View

Any view

Parameter

acl-number: the number of basic ACL, ranging from 2000 to 2999.
acl-name: the basic ACL name introduced via names.
verbose: With the parameter, this command displays the verbose information of both the active and inactive routes that passed filtering rules. Without the parameter, this command only displays the summary of the active routes that passed filtering rules.
Description

Using `display ip routing-table acl` command, you can view the route filtered through specified basic access control list (ACL).

This command is used in track display of route policy to display the route that passed the filtering rule according the input basic ACL number or name.

The command is only applicable to display the route that passed basic ACL filtering rules.

Example

# Display the summary of active routes that are filtered through basic acl 2000.

```
[Quidway] acl number 2000
[Quidway-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.255
[Quidway-acl-basic-2000] rule deny source any
[Quidway-acl-basic-2000] display ip routing-table acl 2000
```

Routes matched by access-list 2000:

Summary count: 4

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Protocol</th>
<th>Pre</th>
<th>Cost</th>
<th>Nexthop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.0/24</td>
<td>DIRECT</td>
<td>0</td>
<td>0</td>
<td>10.1.1.2</td>
<td>Vlan-interface1</td>
</tr>
<tr>
<td>10.1.1.2/32</td>
<td>DIRECT</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoopBack0</td>
</tr>
</tbody>
</table>

For detailed description of the output information, see Table 2-4.

# Display the verbose information of the active and inactive routes that are filtered through basic acl 2000.

```
<Quidway> display ip routing-table acl 2000 verbose
```

Routes matched by access-list 2000:

Summary count: 2

<table>
<thead>
<tr>
<th><strong>Destination: 10.1.1.0</strong></th>
<th>Mask: 255.255.255.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol: #DIRECT</td>
<td>Preference: 0</td>
</tr>
<tr>
<td>*NextHop: 10.1.1.2</td>
<td>Interface: 10.1.1.2(Vlan-interface1)</td>
</tr>
<tr>
<td>Vlinkindex: 0</td>
<td>State: &lt;Int ActiveU Retain Unicast&gt;</td>
</tr>
<tr>
<td>Age: 7:24</td>
<td>Cost: 0/0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Destination: 10.1.1.2</strong></th>
<th>Mask: 255.255.255.255</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol: #DIRECT</td>
<td>Preference: 0</td>
</tr>
<tr>
<td>*NextHop: 127.0.0.1</td>
<td>Interface: 127.0.0.1(InLoopBack0)</td>
</tr>
<tr>
<td>Vlinkindex: 0</td>
<td>State: &lt;NoAdvise Int ActiveU Retain Gateway Unicast&gt;</td>
</tr>
</tbody>
</table>
Table 2-5 Description of information generated by the command `display ip routing-table acl verbose`

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Destination address</td>
</tr>
<tr>
<td>Mask</td>
<td>Mask</td>
</tr>
<tr>
<td>Protocol</td>
<td>Routing protocol</td>
</tr>
<tr>
<td>Preference</td>
<td>Routing preference</td>
</tr>
<tr>
<td>Nexthop</td>
<td>Next hop address</td>
</tr>
<tr>
<td>Interface</td>
<td>Output interface, through which the data packet destined for the destination network segment is sent</td>
</tr>
<tr>
<td>Vlinkindex</td>
<td>Virtual link index</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>State</td>
<td>Route state description:</td>
</tr>
<tr>
<td>ActiveU</td>
<td>The route is selected and is optimum</td>
</tr>
<tr>
<td>Blackhole</td>
<td>Blackhole route is similar to Reject route, but it will not send the ICMP unreachable message to the source end</td>
</tr>
<tr>
<td>Delete</td>
<td>The route is deleted</td>
</tr>
<tr>
<td>Gateway</td>
<td>Identifies that the route is not an interface route</td>
</tr>
<tr>
<td>Hidden</td>
<td>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</td>
</tr>
<tr>
<td>Holddown</td>
<td>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.</td>
</tr>
<tr>
<td>Int</td>
<td>The route is discovered by interior gateway protocol (IGP).</td>
</tr>
<tr>
<td>NoAdvise</td>
<td>The routing protocol does not redistribute NoAdvise route when it redistributes routes based on the policy.</td>
</tr>
<tr>
<td>NotInstall</td>
<td>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.</td>
</tr>
<tr>
<td>Reject</td>
<td>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.</td>
</tr>
<tr>
<td>Retain</td>
<td>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.</td>
</tr>
<tr>
<td>Static</td>
<td>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.</td>
</tr>
<tr>
<td>Unicast</td>
<td>Unicast route</td>
</tr>
</tbody>
</table>
2.1.7 **display ip routing-table ip_address**

**Syntax**

```
display ip routing-table ip_address [ mask ] [ longer-match ] [ verbose ]
```

**View**

Any view

**Parameter**

*ip_address*: Destination IP address.

*mask*: IP address mask, length in dotted decimal notation or integer. It ranges from 0 to 32 when it is expressed with integer.

*verbose*: With the *verbose* parameter, this command displays the verbose information of both the active and inactive routes. Without the parameter, this command only displays the summary of active routes.

*longer-match*: Address route matching the destination address in natural mask range.

**Description**

Using **display ip routing-table ip_address** command, you can view the routing information of the specified destination address.

With different parameters, the output of command is different. The following is the output description for different forms of this command:

- **display ip routing-table ip_address**
  
  If destination address, *ip_address*, has 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.

- **display ip routing-table ip_address mask**,
  
  This command only displays the route fully matching with specified destination address and mask.

- **display ip routing-table ip_address longer-match**
  
  This command displays all destination address route matching with destination address in natural mask range.

**Example**

```
# There is a corresponding route in the natural mask range. Display the summary.

```
<Quidway> display ip routing-table 169.0.0.0
Routing Tables:
    Summary count:1
    Destination/Mask      Protocol Pre Cost Nexthop     Interface
    169.0.0.0/16          Static  60 0 2.1.1.1       LoopBack1
```

For detailed description of the output information, see Table 2-4.

# There is no corresponding route (only the longest matching route is displayed) in natural mask range and summary is displayed.

```
<Quidway> display ip routing-table 169.253.0.0
Routing Tables:
    Summary count:1
    Destination/Mask      Protocol Pre Cost Nexthop     Interface
    169.0.0.0/8           Static  60 0 2.1.1.1       LoopBack1
```

# There are corresponding routes in the natural mask range. Display the detailed information.

```
<Quidway> display ip routing-table 169.0.0.0 verbose
Routing Tables:
    Generate Default: no
    + = Active Route, - = Last Active, # = Both = Next hop in use
    Summary count:2
    **Destination: 169.0.0.0  Mask: 255.0.0.0
        Protocol: #Static        Preference: 60
        *NextHop: 2.1.1.1        Interface: 2.1.1.1(LoopBack1)
        Vlinkindex: 0
        State: <Int ActiveU Static Unicast>
        Age: 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: 3:47    Cost: 0/0
```

# There are no corresponding routes in the natural mask range (only displaying the longest matched route). Display the detailed information.

```
<Quidway> display ip routing-table 169.253.0.0 verbose
Routing Tables:
    Generate Default: no
    + = Active Route, - = Last Active, # = Both = Next hop in use
    Summary count:1
```
**Destination:** 169.0.0.0  **Mask:** 255.0.0.0  
**Protocol:** #Static  **Preference:** -60  
*NextHop:* 2.1.1.1  
Vlinkindex: 0  
State: <Int ActiveU Static Unicast>  
Age: 3:47  **Cost:** 0/0

For detailed description of the output information, see Table 2-5.

### 2.1.8 display ip routing-table ip_address1 ip_address2

**Syntax**

`display ip routing-table ip_address1 mask1 ip_address2 mask2 [verbose ]`

**View**

Any view

**Parameter**

- `ip_address1, ip_address2`: Destination IP address in dotted decimal notation. `ip_address1` and `ip_address2` determine one address range together to display the route in this address range. `ip_address1 anding with mask1 specifies the start of the range while ip_address2 anding with mask2 specifies the end.`
- `mask1, mask2`: IP address mask, length in dotted decimal notation or integer form. It ranges from 0 to 32 when it is presented in integer.
- `verbose`: With the `verbose` parameter, this command displays the verbose information of both the active and inactive routes. Without the parameter, this command only displays the summary of active routes.

**Description**

Using `display ip routing-table ip_address1 ip_address2` command, you can view the route information in the specified address range.

**Example**

# Display the routing information of destination addresses ranging from 1.1.1.0 to 2.2.2.0.

<Quidway>display ip routing-table 1.1.1.0 24 2.2.2.0 24  
Routing tables:  
Summary count: 3  

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Protocol</th>
<th>Pre</th>
<th>Cost</th>
<th>NextHop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.0/24</td>
<td>DIRECT</td>
<td>0</td>
<td>0</td>
<td>1.1.1.1</td>
<td>Vlan-interface1</td>
</tr>
<tr>
<td>1.1.1.1/32</td>
<td>DIRECT</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoopBack0</td>
</tr>
<tr>
<td>2.2.2.0/24</td>
<td>DIRECT</td>
<td>0</td>
<td>0</td>
<td>2.2.2.1</td>
<td>Vlan-interface2</td>
</tr>
</tbody>
</table>

Huawei Technologies Proprietary
2.1.9  display ip routing-table ip-prefix

Syntax

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

View

Any view

Parameter

- `ip-prefix-name`: ip prefix list name.
- `verbose`: With the parameter, this command displays the verbose information of both the active and inactive routes that passed filtering rules. Without the parameter, this command displays the summary of the active routes that passed filtering rules.

Description

Using `display ip routing-table ip-prefix` command, you can view the route information that passed the filtering rule according the input ip prefix list name.

If there is no specified address prefix list, this command will display the verbose information of all active and inactive routes with the parameter `verbose` and it will display the summary of all active routes without the parameter `verbose`.

Example

# Display the summary of the active route that is filtered ip prefix list abc2.

```bash
[Quidway] ip ip-prefix abc2 permit 10.1.1.0 24 less-equal 32
[Quidway] display ip routing-table ip-prefix abc2
```

Routes matched by ip-prefix abc2:

```
Summary count: 2

Destination/Mask  Protocol Pre Cost   Nexthop            Interface
10.1.1.0/24      DIRECT  0 0       10.1.1.2          Vlan-interface1
10.1.1.2/32      DIRECT  0 0       127.0.0.1         InLoopBack0
```

For detailed description of the output information, see Table 2-4.

# Display the verbose info of the active and inactive route that are filtered prefix list abc2.

```bash
[Quidway] display ip routing-table ip-prefix abc2 verbose
```

Routes matched by ip-prefix abc2:

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

Summary count: 2
```

Huawei Technologies Proprietary
2.1.10 display ip routing-table protocol

Syntax

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

View

Any view

Parameter

inactive: With the parameter, this command displays the inactive route information. Without the parameter, this command displays the active and inactive route information.

verbose: With the verbose parameter, this command displays the verbose route information. Without the parameter, this command displays the route summary.

protocol: the parameter has multiple selectable values:
  - direct: Display direct connection route information
  - static: Display the static route information.

Description

Using display ip routing-table protocol command, you can view the route information of specified protocol.

Example

# Display all direct connection routes summary.
<Quidway> display ip routing-table protocol direct
**DIRECT Routing tables:**

Summary count: 4

**DIRECT Routing tables status:**<active>:

Summary count: 3

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Protocol</th>
<th>Pre Cost</th>
<th>Nexthop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>20.1.1.1/32</td>
<td>DIRECT</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoopBack0</td>
</tr>
<tr>
<td>127.0.0.0/8</td>
<td>DIRECT</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoopBack0</td>
</tr>
<tr>
<td>127.0.0.1/32</td>
<td>DIRECT</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoopBack0</td>
</tr>
</tbody>
</table>

**DIRECT Routing tables status:**<inactive>:

Summary count: 1

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Protocol</th>
<th>Pre Cost</th>
<th>Nexthop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>210.0.0.1/32</td>
<td>DIRECT</td>
<td>0</td>
<td>127.0.0.1</td>
<td>InLoopBack0</td>
</tr>
</tbody>
</table>

# View the static routing table.

```ansi
<Quidway> display ip routing-table protocol static
```

**STATIC Routing tables:**

Summary count: 1

**STATIC Routing tables status:**<active>:

Summary count: 0

**STATIC Routing tables status:**<inactive>:

Summary count: 1

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Protocol</th>
<th>Pre</th>
<th>Cost</th>
<th>Nexthop</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.3.0/24</td>
<td>STATIC</td>
<td>60</td>
<td>0</td>
<td>1.2.4.5</td>
<td>Vlan-interface1</td>
</tr>
</tbody>
</table>

For detailed description of the output information, see Table 2-4.

### 2.1.11 `display ip routing-table radix`

**Syntax**

```
display ip routing-table radix
```

**View**

Any view

**Parameter**

None

**Description**

Using `display ip routing-table radix` command, you can view the route information in a tree structure.

**Example**

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

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

Table 2-6 Description of information generated by the command display ip routing-table radix

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INET</td>
<td>Address suite</td>
</tr>
<tr>
<td>inodes</td>
<td>Number of nodes</td>
</tr>
<tr>
<td>routes</td>
<td>Number of routes</td>
</tr>
</tbody>
</table>

2.1.12 display ip routing-table statistics

Syntax

display ip routing-table statistics

View

Any view

Parameter

None

Description

Using display ip routing-table statistics command, you can view the integrated routing information.

The integrated routing information includes total route amount, the route amount added or deleted by protocol, amount of the routes that are labeled deleted but not deleted, the active route amount and inactive route amount.

Example

# Display the integrated route information.
<Quidway> display ip routing-table statistics

Routing tables:

<table>
<thead>
<tr>
<th>Proto</th>
<th>route</th>
<th>active</th>
<th>added</th>
<th>deleted</th>
<th>freed</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIRECT</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>STATIC</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Table 2-7 Description of information generated by the command **display ip routing-table statistics**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proto</td>
<td>Routing protocol</td>
</tr>
<tr>
<td>route</td>
<td>Number of routes</td>
</tr>
<tr>
<td>active</td>
<td>Number of active routes</td>
</tr>
<tr>
<td>added</td>
<td>Number of added routes after the router is rebooted or the routing table is cleared last time.</td>
</tr>
<tr>
<td>deleted</td>
<td>Number of deleted routes (such routes will be freed in a period of time)</td>
</tr>
<tr>
<td>freed</td>
<td>Number of freed routes</td>
</tr>
</tbody>
</table>

2.1.13 **display ip routing-table verbose**

**Syntax**

```plaintext
display ip routing-table verbose
```

**View**

Any view

**Parameter**

None

**Description**

Using **display ip routing-table verbose** command, you can view the verbose routing table information.

With the **verbose** parameter, this command displays the verbose routing table information. The descriptor describing the route state will be displayed first, then the statistics of the entire routing table will be output and finally the verbose description of each route will be output.

All current routes, including inactive route and invalid route, can be displayed using **display ip routing-table verbose** command.

**Example**

```plaintext
# Display the verbose routing table information.
<Quidway> display ip routing-table verbose
Routing Tables:
  Generate Default: no
  + = Active Route, - = Last Active, # = Both  * = Next hop in use
```

Huawei Technologies Proprietary
Destinations: 2 Routes: 2
Holddown: 0 Delete: 0 Hidden: 0

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

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

First, display statistics of the whole routing table and then output detailed information of every route entry in turn. The meaning of route status is shown in Table 2-5, and the statistics of routing table is shown in the following table.

Table 2-8 Description of information generated by the command display ip routing-table verbose

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Holddown</td>
<td>Number of held-down routes</td>
</tr>
<tr>
<td>Delete</td>
<td>Number of deleted routes</td>
</tr>
<tr>
<td>Hidden</td>
<td>Number of hidden routes</td>
</tr>
</tbody>
</table>

2.1.14 interface vlan-interface

Syntax

interface vlan-interface vlan-id
undo interface vlan-interface vlan-id

View

System view

Parameter

vlan-id: Specifies the identification of management VLAN interface, ranging from 1 to 4094.
Description

Using **interface vlan-interface** command, you can create and enter management VLAN interface view. Using **undo interface vlan-interface** command, you can cancel management VLAN interface.

Before creating and entering the management VLAN interface view, the corresponding VLAN specified by **vlan-id** must be created.

Example

```plaintext
# Enter the view of management VLAN interface 1.
[Quidway] interface vlan-interface 1
```

### 2.1.15 ip address

**Syntax**

```
ip address ip-address net-mask
undo ip address [ ip-address net-mask ]
```

**View**

VLAN interface view

**Parameter**

- **ip-address**: Configures the IP address of the management VLAN interface.
- **net-mask**: Configures the mask of the management VLAN interface.

**Description**

Using **ip address** command, you can configure the IP address and mask of the management VLAN interface. Using **undo ip address** command, you can cancel the IP address and mask of the management VLAN interface.

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

**Example**

```plaintext
# Configure the IP address and mask for management VLAN interface 20.
[Quidway-Vlan-interface20] ip address 1.1.1.1 255.0.0.0
```

### 2.1.16 ip host

**Syntax**

```
ip host hostname ip-address
undo ip host hostname [ ip-address ]
```

Huawei Technologies Proprietary
View

System view

Parameter

hostname: Name of the host, a character string consisting of 1 to 20 characters, including letters, numbers or "_", and it must contain at least one letter.

ip-address: Specifies the host IP address corresponding to the host name in dotted decimal notation.

Description

Using ip host command, you can configure the host name and corresponding IP address. Using undo ip host command, you can cancel the host name and corresponding IP address.

By default, the host name and corresponding IP address are none.

For the related command, see display ip host.

Example

# Configure the IP address of the host named Lanswitch2 at 10.110.0.2.
[Quidway] ip host Lanswitch2 10.110.0.2

2.1.17 ip route-static

Syntax

ip route-static ip-address { mask | mask-length } { null null-interface-number | gateway-address } [ preference preference-value ]
undo ip route-static ip-address { mask | mask-length } { null null-interface-number | gateway-address } [ preference preference-value ]

View

System view

Parameter

ip-address: Specifies the destination IP address in dotted decimal notation.
mask: Mask.

mask-length: Mask length. Since "1" s in the 32-bit mask are required to be consecutive, the mask in dotted decimal format can be replaced by mask-length, which is the number of the consecutive "1" s in the mask.

null null-interface-number: Specify the NULL interface of the route. The packets sent to NULL interface, a kind of virtual interface, will be discarded at once. Thus this can decrease the system load.
**2.1.18 ip route-static default-preference**

**Syntax**

```
ip route-static default-preference default-preference-value
undo ip route-static default-preference
```

**View**

System view

**Parameter**

`default-preference-value`: The default preference value of static routes, ranging 1 to 255. Its default value is 60.

**Description**

Using `ip route-static default-preference` command, you can configure the default preference value of static routes. Using `undo ip route-static default-preference` command, you can remove the default preference value of static routes configure.

A static route’s preference will be the `default-preference-value` set by this command if its preference is not specified when configured by `ip route-static` command.

For the related commands, see `display ip routing-table, ip route-static`.

---

**Description**

Using `ip route-static` command, you can configure a static route. Using `undo ip route-static` command, you can cancel the configured static route.

By default, the system can obtain the sub-net route directly connected with the router. When configuring a static route, the default preference is 60 if it is not specified.

Precautions: When the destination IP address and the mask are both 0.0.0.0, it is the configured default route. If it fails to detect the routing table, a packet will be forwarded along the default route.

For the related command, see `display ip routing-table`.

**Example**

```
# Configure the next hop of the default route as 129.102.0.2.
[Quidway] ip route-static 0.0.0.0 0.0.0.0 129.102.0.2
```

`gateway-address`: Specifies the next hop IP address (in dotted decimal notation) of the route.

`preference-value`: Specifies the preference of the route, ranging from 1 to 255.
Example

# Configure the default preference of static routes as 120.
[Quidway] ip route-static default-preference 120

2.1.19 shutdown

Syntax

shutdown
undo shutdown

View

VLAN interface view

Parameter

None

Description

Using shutdown command, you can disable the management VLAN interface. Using undo shutdown command, you can enable the management VLAN interface.

By default, when all the Ethernet ports belonging to the management VLAN are in down status, the management VLAN interface is also down, i.e. the management VLAN interface is disabled. When there is one or more Ethernet ports in up status, the management VLAN interface is also up, i.e. the management VLAN interface is enabled.

Example

# Enable the management VLAN interface.
[Quidway-Vlan-interface1] undo shutdown
Table of Contents

Chapter 1 Ethernet Port Configuration Commands.......................................................... 1-1
  1.1 Ethernet Port Configuration Commands................................................................... 1-1
     1.1.1 broadcast-suppression...................................................................................... 1-1
     1.1.2 description................................................................................................. 1-1
     1.1.3 display interface......................................................................................... 1-2
     1.1.4 display loopback-detection......................................................................... 1-5
     1.1.5 display port .............................................................................................. 1-6
     1.1.6 duplex...................................................................................................... 1-7
     1.1.7 flow-constrain ......................................................................................... 1-7
     1.1.8 flow-constrain method............................................................................ 1-8
     1.1.9 flow-control ......................................................................................... 1-9
     1.1.10 flow-interval ...................................................................................... 1-10
     1.1.11 interface ............................................................................................ 1-10
     1.1.12 loopback........................................................................................... 1-11
     1.1.13 loopback-detection control enable ......................................................... 1-12
     1.1.14 loopback-detection enable ................................................................. 1-12
     1.1.15 loopback-detection interval-time ....................................................... 1-13
     1.1.16 loopback-detection per-vlan enable .................................................. 1-14
     1.1.17 mdi..................................................................................................... 1-14
     1.1.18 port access vlan ............................................................................... 1-15
     1.1.19 port hybrid pvid vlan ........................................................................ 1-15
     1.1.20 port hybrid vlan .............................................................................. 1-16
     1.1.21 port link-type .................................................................................. 1-17
     1.1.22 port trunk permit vlan .......................................................... 1-18
     1.1.23 port trunk pvid vlan .................................................................... 1-18
     1.1.24 reset counters interface.................................................................... 1-19
     1.1.25 shutdown ....................................................................................... 1-20
     1.1.26 speed.............................................................................................. 1-20

Chapter 2 Ethernet Port Link Aggregation Commands.................................................... 2-1
  2.1 Ethernet Port Link Aggregation Commands......................................................... 2-1
     2.1.1 display link-aggregation .................................................................... 2-1
     2.1.2 link-aggregation ............................................................................. 2-2

Huawei Technologies Proprietary
Chapter 1 Ethernet Port Configuration Commands

1.1 Ethernet Port Configuration Commands

1.1.1 broadcast-suppression

Syntax

    broadcast-suppression ratio
    undo broadcast-suppression

View

    Ethernet port view

Parameter

    ratio: Specifies the maximum wire speed ratio of the broadcast traffic allowed on the port. The value ranges from 1 to 100. By default, the value is 100. The smaller the ratio is, the smaller the broadcast traffic is allowed.

Description

Using broadcast-suppression command, you can configure the broadcast traffic size enabled on port. Once the broadcast traffic exceeds the value set by the user, the system will discard some broadcast to ensure network service so that the traffic ratio of broadcast is maintained in a proper range. Using undo broadcast-suppression command, you can restore the default broadcast traffic enabled on port as 100. i.e., 100% broadcast traffic is allowed to pass through.

Example

    # Enable 20% broadcast cast to pass, i.e. 80% broadcast storm suppression is made on broadcast traffic of port.
    [Quidway-Ethernet0/1] broadcast-suppression 20

1.1.2 description

Syntax

    description text
    undo description
View

Ethernet port view

Parameter

text: Port description character string, with 80 characters at most.

Description

Using description command, you can configure the description character string for Ethernet port. Using undo description command, you can cancel the port description character string.

By default, the port description character string is null.

Example

# Configure the description character string of Ethernet port Ethernet0/1 as lanswitch-interface.
[Quidway-Ethernet0/1] description lanswitch-interface

1.1.3 display interface

Syntax

display interface [ interface_type | interface_type interface_num | interface_name ]

View

Any 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

Using display interface command, you can view the configuration information on the port.

If the port type and number are not specified when displaying the port information, the information of all the ports will be displayed. If only the port type is specified, all the information of the ports of this type will be displayed. If both port type and port number are specified, the information of the designated port will be displayed.
Example

# Display configuration information of Ethernet0/12.

<Quidway> display interface ethernet0/12
Ethernet0/12 current state : DOWN
  IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc01-0101
  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 force link, link duplex type is force link
  Flow-control is enabled
  Value of flow-constrain is: 111 bps
  Process method when overflow the constraint is: send trap
  Period of flow-constrain detection is: 20
  The Maximum Frame Length is 1536
  Broadcast MAX-ratio: 100%
  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
    0 broadcasts, 0 multicasts
  Input(normal): - packets, - bytes
    - broadcasts, - multicasts
  Input: 0 input errors, 0 runts, 0 giants, - throttles, 0 CRC
    0 frame, - overruns, 0 aborts, 0 ignored, - parity errors
  Output(total): 0 packets, 0 bytes
    0 broadcasts, 0 multicasts, 0 pauses
  Output(normal): - packets, - bytes
    - broadcasts, - multicasts, - pauses
  Output: 0 output errors, - underruns, - buffer failures
    0 aborts, 0 deferred, 0 collisions, 0 late collisions
    0 lost carrier, - no carrier
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet0/12 current state</td>
<td>The current state of Ethernet port (UP or DOWN)</td>
</tr>
<tr>
<td>IP Sending Frames’ Format</td>
<td>Ethernet frame format</td>
</tr>
<tr>
<td>Hardware address</td>
<td>Port hardware address</td>
</tr>
<tr>
<td>Description</td>
<td>Port description character string</td>
</tr>
<tr>
<td>The Maximum Transmit Unit</td>
<td>Maximum transmit unit</td>
</tr>
<tr>
<td>Media type</td>
<td>Type of media</td>
</tr>
<tr>
<td>loopback not set</td>
<td>Port loopback test state</td>
</tr>
<tr>
<td>Port hardware type</td>
<td>Port hardware type</td>
</tr>
<tr>
<td>100Mbps-speed mode, full-duplex mode</td>
<td>Both the duplex mode and the rate are set to auto-negotiation. The rate of 100Mbps and the mode of full-duplex are adopted after negotiating with its peer</td>
</tr>
<tr>
<td>Link speed type is autonegotiation, link duplex type is autonegotiation</td>
<td></td>
</tr>
<tr>
<td>Flow-control is enabled</td>
<td>Port flow control is enabled.</td>
</tr>
<tr>
<td>Value of flow-constrain</td>
<td>Traffic threshold on the port</td>
</tr>
<tr>
<td>Process method when overflow the constraint</td>
<td>Handling pattern when actual traffic on the port exceeds the threshold</td>
</tr>
<tr>
<td>Period of flow-constrain detection</td>
<td>Time interval to detect traffic on the port</td>
</tr>
<tr>
<td>The Maximum Frame Length</td>
<td>Maximum length of the Ethernet frames that can pass through the port</td>
</tr>
<tr>
<td>Broadcast MAX-ratio</td>
<td>Port broadcast storm suppression ratio</td>
</tr>
<tr>
<td>PVID</td>
<td>Port default VLAN ID</td>
</tr>
<tr>
<td>Mdi type</td>
<td>Cable type</td>
</tr>
<tr>
<td>Port link-type</td>
<td>Port link type</td>
</tr>
<tr>
<td>Tagged VLAN ID</td>
<td>The VLANs with packets tagged</td>
</tr>
<tr>
<td>Untagged VLAN ID</td>
<td>The VLANs with packets untagged</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Last 300 seconds input: 0 packets/sec 0 bytes/sec</td>
<td>The input/output rate and the passing packet number on this port in the last 300 seconds</td>
</tr>
<tr>
<td>Last 300 seconds output: 0 packets/sec 0 bytes/sec</td>
<td></td>
</tr>
<tr>
<td>input(total): 0 packets, 0 bytes 0 broadcasts, 0 multicasts</td>
<td>The statistics information of input/output packets and errors on this port</td>
</tr>
<tr>
<td>input(normal): - packets, - bytes - broadcasts, - multicasts</td>
<td></td>
</tr>
<tr>
<td>input: 0 input errors, 0 runts, 0 giants, - throttles, 0 CRC</td>
<td></td>
</tr>
<tr>
<td>- frame, - overruns, 0 aborts, 0 ignored, - parity errors</td>
<td></td>
</tr>
<tr>
<td>Output(total): 0 packets, 0 bytes 0 broadcasts, 0 multicasts, 0 pauses</td>
<td></td>
</tr>
<tr>
<td>Output(normal): - packets, - bytes - broadcasts, - multicasts, - pauses</td>
<td></td>
</tr>
<tr>
<td>Output: 0 output errors, 0 underruns, - buffer failures - aborts, 0 deferred, 0 collisions, 0 late collisions - lost carrier, - no carrier</td>
<td></td>
</tr>
</tbody>
</table>

1.1.4 display loopback-detection

Syntax

```
display loopback-detection
```

View

Any view

Parameter

`none`
Using `display loopback-detection` command, you can 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**

```
# Display if the port loopback detection is enabled.
<Quidway> display loopback-detection
Loopback-detection is running
Detection interval time is 30 seconds
There is no port existing loopback link
```

**Table 1-2 Output description of the display loopback-detection command**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loopback-detection is running</td>
<td>The loopback detection is enabled</td>
</tr>
<tr>
<td>Detection interval time is 30 seconds</td>
<td>The detection interval is 30 seconds</td>
</tr>
<tr>
<td>There is no port existing loopback link</td>
<td>No port is in the loopback state</td>
</tr>
</tbody>
</table>

1.1.5 `display port`

**Syntax**

`display port { hybrid | trunk }
```

**View**

Any view

**Parameter**

- **hybrid**: Display Hybrid port.
- **Trunk**: Display Trunk port.

**Description**

Using `display port` command, you can view the ports in the current system, whose link type is Hybrid or Trunk. If there is any such port, display the corresponding port name.

**Example**

```
# Display the Hybrid ports in the current system.
<Quidway> display port hybrid
```
Now, the following hybrid ports exist:

- Ethernet0/1
- Ethernet0/2

The above information displays that the current system has two Hybrid ports, Ethernet0/1 and Ethernet0/2.

### 1.1.6 duplex

**Syntax**

```
duplex { auto | full | half }
undo duplex
```

**View**

Ethernet port view

**Parameter**

- **auto**: Port auto-negotiation attribute.
- **full**: Port full-duplex attribute.
- **half**: Port half-duplex attribute.

**Description**

Using **duplex** command, you can configure the full-duplex/half-duplex attribute of the Ethernet port. Using **undo duplex** command, you can restore the duplex attribute of the port to default auto-negotiation mode.

By default, the duplex attribute is **auto**.

For the related command, see **speed**.

**Example**

```
# Configure the Ethernet port Ethernet0/1 as auto-negotiation attribute.
[Quidway-Ethernet0/1] duplex auto
```

### 1.1.7 flow-constrain

**Syntax**

```
flow-constrain time-value flow-value { bps | pps }
undo flow-constrain time-value flow-value { bps | pps }
```

**View**

Ethernet port view
Parameter

*time-value*: Time interval to detect traffic on the port, ranging from 5 to 300 (seconds) and in steps of 5.

*flow-value*: Traffic threshold on the port, in the range of 0 to 4294967295. It defaults to 0.

*bps*: Bytes per second.

*pps*: Packets per second.

Description

Use the `flow-constrain` command to define traffic threshold on the port.

Use the `undo flow-constrain` command to remove the traffic threshold configuration on the port.

By default, no traffic threshold is defined on the port.

After you define traffic threshold and handling pattern on the port, the system detects and counts the traffic in a specified interval. If the actual traffic exceeds the threshold, the system handles the port based on the defined pattern.

Example

```plaintext
# Configure the traffic threshold on the Ethernet0/1 port as 5000pps and detection interval as 10 seconds.
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] interface ethernet0/1
[Quidway-Ethernet0/1] flow-constrain 10 5000 pps
```

1.1.8 flow-constrain method

Syntax

`flow-constrain method { shutdown | trap }
undo flow-constrain method`

View

Ethernet port view

Parameter

*shutdown*: Disables the port and sends trap messages.

*trap*: Sends trap messages only.
Description

Use the `flow-constrain method` command to define handling pattern when actual traffic on the port exceeds the threshold.

Use the `undo flow-constrain` command to restore the default handling pattern.

By default, only trap messages are sent when actual traffic on the port exceeds the threshold.

Example

```
# Configure the system to disable the port and send trap messages when actual traffic on the port exceeds the threshold.
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] interface ethernet0/1
[Quidway-Ethernet0/1] flow-constrain method shutdown
```

1.1.9 flow-control

Syntax

```
flow-control
undo flow-control
```

View

Ethernet port view

Parameter

`none`

Description

Using `flow-control` command, you can enable flow control feature on the Ethernet port to avoid discarding data packets due to congestion. Using `undo flow-control` command, you can disable flow control feature.

By default, flow control on the Ethernet port is disabled.

Example

```
# Enable flow control on Ethernet0/1.
[Quidway-Ethernet0/1] flow-control
```
1.1.10 flow-interval

Syntax

flow-interval interval
undo flow-interval

View

Ethernet port view

Parameter

interval: Specifies time interval, ranging from 5 to 300 in seconds. The step is 5. The default value is 300.

Description

Using the flow-interval command, you can configure a time interval. When calculating port statistics information, the switch calculates the average port speed during the time interval. Using the undo flow-interval command, you can restore the default value.

For the related command, see display interface.

Example

# Configure the time interval to 100 seconds on Ethernet0/1.
[Quidway-Ethernet0/1] flow-interval 100

1.1.11 interface

Syntax

interface { interface_type interface_num | interface_name }

View

System view

Parameter

interface_type: Specifies the port type. It can be Ethernet, or GigabitEthernet.

interface_num: Port number. It adopts slot number/port number format. For S3026C/S3026C-PWR, the slot number ranges from 0 to 2. Slot 0 contains the fixed Ethernet ports provided by the switch and the port number ranges from 1 to 24. Slot 1 or 2 contains the extended Ethernet ports provided by the two extended modules on front panel and the port number can be 1 only. For S3026G and S3026T switches, the slot number ranges from 0 to 2. Slot 0 contains the fixed Ethernet ports provided by the switch and the port number ranges from 1 to 24. Slot 1 or 2 contains the two uplink Ethernet ports provided by the switch and the port number can be 1 only.
For S3026E FM and S3026E FS Ethernet Switches, the slot number ranges from 0 to 4. Slot 0 contains the fixed Ethernet ports provided by the switch and the port number ranges from 1 to 6. Slot 1 or 2 contains the extended Ethernet ports provided by the two extended modules in the front panel and the port number ranges from 1 to 6. Slot 3 or 4 represents the extended Ethernet ports provided by the two extended modules on the rear panel and the port number can only be 1.

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

Description

Using interface command, you can enter the Ethernet port view.

If the user wants to configure the related parameters of the Ethernet port, he must first use this command to enter the Ethernet port view.

Example

# Enter the Ethernet0/1 port view.
[Quidway] interface ethernet0/1

1.1.12 loopback

Syntax

loopback { external | internal }

View

Ethernet port view

Parameter

external: External loop test.
internal: Internal loop test.

Description

Using loopback command, you can configure the Ethernet port to perform the loopback test to check whether the Ethernet port works normally and the loop test will finish automatically after being performed for a while.

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

Example

# Perform the internal loop test for Ethernet0/1.
[Quidway-Ethernet0/1] loopback internal
1.1.13 loopback-detection control enable

Syntax

```
loopback-detection control enable
undo loopback-detection control enable
```

View

System view/Ethernet port view

Parameter

none

Description

Using the command, you can enable loopback detection controlled function on Trunk and Hybrid port, that is, when the system finds out that ports on a certain VLAN on Trunk or Hybrid port is looped back, it then makes the Trunk and Hybrid port operate under control, meantime, deletes the port corresponding MAC address entry. Using the `undo loopback-detection control enable` command, you can disable this function, that is, when the system finds out that port on a certain VLAN on Trunk or Hybrid port is looped back, it only reports the Trap information. The Trunk or Hybrid port is still operates in the normal state.

By default, loopback detection controlled function on Trunk or Hybrid port is enabled.

Note that, this command has no effect on Access ports.

Example

```
# Enable the port loopback detection controlled function.
[Quidway] loopback-detection control enable
```

1.1.14 loopback-detection enable

Syntax

```
loopback-detection enable
undo loopback-detection enable
```

View

System view/Ethernet port view

Parameter

none
Description

Using **loopback-detection enable** command, you can enable the port loopback detection. If there is a loopback port found, the switch will put it under control. Using **undo loopback-detection enable** command, you can disable the port loopback detection.

Using this command in the system, you can enable/disable the port loopback detection function of the entire device; using this command in Ethernet port view, you can enable/disable the port loopback detection function of the current port.

By default, port loopback detection is enabled.

For the related command, see **display loopback-detection**.

Example

```
# Enable the port loopback detection.
[Quidway] loopback-detection enable
```

### 1.1.15 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**

Using **loopback-detection interval-time** command, you can configure detection interval for the external loopback condition of each port. Using **undo loopback-detection interval-time** command, you can restore the default interval.

For the related command, see **display loopback-detection**.

**Example**

```
# Configure the detection interval for the external loopback condition of each port to 10 seconds.
[Quidway] loopback-detection interval-time 10
```
1.1.16  loopback-detection per-vlan enable

Syntax

```
loopback-detection per-vlan enable
undo loopback-detection per-vlan enable
```

View

```
Ethernet port view
```

Parameter

```
none
```

Description

Using the `loopback-detection per-vlan enable` command, you can configure that the system performs loopback detection to all VLANs on Trunk and Hybrid ports. Using the `undo loopback-detection per-vlan enable` command, you can configure that the system only performs loopback detection to the default VLANs on the port.

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

Example

```
# Configure the detection interval for the external loopback condition of each port to 10 seconds.
[Quidway-Ethernet0/1] loopback-detection per-vlan enable
```

1.1.17  mdi

Syntax

```
mdi { across | auto | normal }
undo mdi
```

View

```
Ethernet port view
```

Parameter

```
across: The network cable type is cross-over cable.
auto: The network cable will be recognized whether it is straight-through cable or cross-over cable.
```

normal: The network cable of the port is straight-through cable.
Description

Using `mdi` command, you can configure the network cable type of the Ethernet ports. Using `undo mdi` command, you can restore the default type.

By default, the network cable type will be recognized automatically.

Note that this command only has effect 10/100Base-TX and 1000Base-T ports.

Example

# Configure the network cable type of Ethernet port Ethernet0/1 as auto.
  [Quidway-Ethernet0/1] mdi auto

1.1.18 port access vlan

Syntax

```
port access vlan vlan_id
undo port access vlan
```

View

Ethernet port view

Parameter

- `vlan_id`: VLAN ID defined in IEEE802.1Q, ranging from 2 to 4094.

Description

Using `port access vlan` command, you can join the access port to a specified VLAN. Using `undo port access vlan` command, you can cancel the access port from the VLAN.

The use condition of this command is the VLAN indicated in `vlan_id` must exist.

Example

# Join Ethernet0/1 port to VLAN3 (VLAN3 has existed).
  [Quidway-Ethernet0/1] port access vlan 3

1.1.19 port hybrid pvid vlan

Syntax

```
port hybrid pvid vlan vlan_id
undo port hybrid pvid
```

View

Ethernet port view
Parameter

- **vlan_id**: VLAN ID defined in IEEE802.1Q, ranging from 1 to 4094 and the default `vlan_id` is 1.

Description

Using **port hybrid pvid vlan** command, you can configure the default VLAN ID of the hybrid port. Using **undo port hybrid pvid** command, you can 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 shall be consistent with that of the peer one, otherwise, the packet cannot be properly transmitted.

For the related command, see **port link-type**.

Example

```
# Configure the default VLAN of the hybrid port Ethernet0/1 to 100.
[Quidway-Ethernet0/1] port hybrid pvid vlan 100
```

### 1.1.20 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`: `vlan_id_list = [ vlan_id1 [ to vlan_id2 ] ]&<1-10>` specifies which VLAN the hybrid port will be added to. It can be discrete. The `vlan_id` ranges from 1 to 4094. &<1-10> indicates that the former parameter can be input 10 times repeatedly at most.

- **tagged**: The packet of specified VLAN will have tag.
- **untagged**: The packet of specified VLAN will not have tag.

**Description**

Using **port hybrid vlan** command, you can join the hybrid port to specified existing VLAN. Using **undo port hybrid vlan** command, you can cancel the hybrid port from the specified VLAN.
Hybrid port can belong to multiple VLANs. If the **port hybrid vlan vlan_id_list { tagged | untagged }** command is used for many times, the VLANs carried by the hybrid port is the set of **vlan_id_list**.

This command can be used on condition that the VLAN specified with **vlan_id** must have been existed.

For the related command, see **port link-type**.

**Example**

```
# Join hybrid port Ethernet0/1 to VLAN of 2, 4 and 50-100, and these VLAN will have tags.
[Quidway-Ethernet0/1] port hybrid vlan 2 4 50 to 100 tagged
```

### 1.1.21 port link-type

**Syntax**

```
port link-type { access | hybrid | trunk }
undo port link-type
```

**View**

Ethernet port view

**Parameter**

- **access**: Configure the port as access port.
- **hybrid**: Configure the port as hybrid port.
- **trunk**: Configure the port as trunk port

**Description**

Using **port link-type** command, you can configure the link type of Ethernet port. Using **undo port link-type** command, you can restore the port as default status, i.e. access port.

You can configure three types of ports concurrently on the same switch, but you cannot switch between trunk port and hybrid port. You must turn it first into access port and then set it as other type. For example, you cannot configure a trunk port directly as hybrid port, but first set it as access port and then as hybrid port.

By default, the port is access port.

**Example**

```
# Configure Ethernet port Ethernet0/1 as trunk port.
[Quidway-Ethernet0/1] port link-type trunk
```
1.1.22 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_list: vlan_id_list = [ vlan_id1 [ to vlan_id2 ] ]&<1-10> is the VLAN range joined by the trunk port. It can be discrete. The vlan_id ranges from 2 to 4094. &<1-10> indicates that the former parameter can be input 10 times repeatedly at most.
    all: Join the trunk port to all VLANs.

Description

Using **port trunk permit vlan** command, you can join trunk port to specified VLAN. Using **undo port trunk permit vlan** command, you can cancel trunk port from specified VLAN.

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**.

This command can be used on condition that the VLAN specified with **vlan_id** is not the default one.

For the related command, see **port link-type**.

Example

    # Join the trunk port Ethernet0/1 to VLAN 2, 4 and 50-100.
    [Quidway-Ethernet0/1] port trunk permit vlan 2 4 50 to 100

1.1.23 port trunk pvid vlan

Syntax

    port trunk pvid vlan vlan_id
    undo port trunk pvid

View

    Ethernet port view
Parameter

*vlan_id*: VLAN ID defined in IEEE802.1Q, ranging from 1 to 4094 and the default *vlan_id* is 1.

Description

Using **port trunk pvid vlan** command, you can configure the default VLAN ID of trunk port. Using **undo port trunk pvid** command, you can restore the default VLAN ID of the port.

Trunk port and isolate-user-vlan cannot be configured simultaneously.

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

For the related command, see **port link-type**.

Example

```
# Configure the default VLAN of the trunk port Ethernet0/1 to 100.
[Quidway-Ethernet0/1] port trunk pvid vlan 100
```

1.1.24 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

Using **reset counters interface** command, you can reset the statistical information on the port and count the related information again on the port for the user.

If the port type and number are not specified when clearing the port information, information of all ports on the switch will be cleared. If only the port type is specified, all the information on the ports of this type will be cleared. If both port type and port number are specified, the information on the designated port will be cleared.
1.1.25 shutdown

Syntax

shutdown
undo shutdown

View

Ethernet port view

Parameter

none

Description

Using shutdown command, you can disable the Ethernet port. Using undo shutdown command, you can enable the Ethernet port.

By default, the Ethernet port is enabled.

Example

# Enable Ethernet port Ethernet0/1.
[Quidway-Ethernet0/1] undo shutdown

1.1.26 speed

Syntax

- For 100M Ethernet port, this command is in the following format:
  speed \{ 10 | 100 | auto \}
- For 1000M Ethernet port, this command is in the following format:
  speed \{ 10 | 100 | 1000 | auto \}
- The undo form of this command is:
  undo speed

View

Ethernet port view

Example

# Reset statistical information on Ethernet port Ethernet0/1.
<Quidway> reset counters interface ethernet0/1


Parameter

- **10**: The speed on the port is 10Mbps.
- **100**: The speed on the port is 100Mbps.
- **1000**: The speed on the port is 1000Mbps.
- **auto**: The port speed is in peer auto-negotiation status.

Description

Using `speed` command, you can configure the port speed. Using `undo speed` command, you can restore the default speed.

By default, the speed is **auto**.

For the related command, see `duplex`.

Example

```
# Configure Ethernet port Ethernet0/1 port speed as 10Mbps.
[Quidway-Ethernet0/1] speed 10
```
Chapter 2 Ethernet Port Link Aggregation Commands

2.1 Ethernet Port Link Aggregation Commands

2.1.1 display link-aggregation

Syntax

display link-aggregation [ master_port_num ]

View

Any view

Parameter

master_port_num: Master port number in an aggregation port group.

Description

Using display link-aggregation command, you can view the related information on aggregation port.

If the master port number of an aggregation is specified, information on this link aggregation will be displayed. If the master port number is not specified, information of all link aggregations will be displayed.

For the related command, see link-aggregation.

Example

# Display the related information of the aggregation group with the master port number as Ethernet0/1.
<Quidway> display link-aggregation ethernet0/1
Master port: Ethernet0/1
Other sub-ports:
    Ethernet0/2
Mode: both

Table 2-1 The description of link aggregation

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master port</td>
<td>Master port</td>
</tr>
</tbody>
</table>
### 2.1.2 link-aggregation

**Syntax**

```markdown
link-aggregation port_num1 to port_num2 { both | ingress }
undo link-aggregation { master_port_num | all }
```

**View**

System view

**Parameter**

- `port_num1`: Starting range value of Ethernet port joined the Ethernet link aggregation.
- `port_num2`: Last range value of Ethernet port joined the Ethernet link aggregation.
- `both`: Configures that the sub-ports in the link aggregation share outgoing load on the port depending on the source address and destination MAC address.
- `ingress`: Configures that the sub-ports in the link aggregation share outgoing load on the port depending on the source MAC addresses.
- `master_port_num`: Master port number in link aggregation.
- `all`: all aggregated ports.

**Description**

Using `link-aggregation` command, you can configure a series of ports to aggregation port and the port with the smallest port number as master port. Using `undo link-aggregation` command, you can cancel the Ethernet link aggregation.

Note that the Ethernet ports to be aggregated can not work in auto-negotiation mode and must work in the same mode, which can be 10M_FULL (10Mbps speed, full duplex), 100M_FULL (100Mbps speed, full duplex), or 1000M_FULL (1000Mbps speed, full duplex), otherwise, they cannot be aggregated.

For the related command, see `display link-aggregation`.

**Example**

```markdown
# Configure outgoing load balance on the port depending on the source and destination MAC addresses.
[Quidway] link-aggregation ethernet0/1 to ethernet0/2 both
```
# Table of Contents

## Chapter 1 VLAN Configuration Commands

1.1 VLAN Configuration Commands

1.1.1 description

1.1.2 display vlan

1.1.3 port

1.1.4 vlan

1.1.5 vlan { enable | disable }

## Chapter 2 Isolate-User-Vlan Configuration Commands

2.1 isolate-user-vlan Configuration Commands

2.1.1 display isolate-user-vlan

2.1.2 isolate-user-vlan

2.1.3 isolate-user-vlan enable

2.1.4 isolate-user-vlan igsp enable

## Chapter 3 GARP/GVRP Configuration Commands

3.1 GARP Configuration Commands

3.1.1 display garp statistics

3.1.2 display garp timer

3.1.3 garp timer

3.1.4 garp timer leaveall

3.1.5 reset garp statistics

3.2 GVRP Configuration Command

3.2.1 display gvrp statistics

3.2.2 display gvrp status

3.2.3 gvrp

3.2.4 gvrp registration

## Chapter 4 Voice VLAN Configuration Commands

4.1 Voice VLAN Configuration Commands

4.1.1 display voice vlan oui

4.1.2 display voice vlan status

4.1.3 voice vlan aging

4.1.4 voice vlan enable

4.1.5 voice vlan

4.1.6 voice vlan mac-address

4.1.7 voice vlan mode

4.1.8 voice vlan security enable
Chapter 1  VLAN Configuration Commands

1.1  VLAN Configuration Commands

1.1.1  description

Syntax

description string

undo description

View

VLAN view

Parameter

string: description character string of current VLAN, with a length ranging from 1 to 32 characters. The default description character string of current VLAN is VLAN ID of the VLAN, e.g. VLAN 0001.

Description

Using description command, you can configure a description for the current VLAN. Using undo description command, you can restore the default description of current VLAN.

For the related command, see display vlan.

Example

# Specify a description character string “RESEARCH” for current VLAN.

[Quidway-vlan1] description RESEARCH

1.1.2  display vlan

Syntax

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

Any view

Parameter

\texttt{vlan\_id}: Display information of specified VLAN.

\texttt{all}: Display information of all VLANs.

\texttt{static}: Display information of VLAN created statically by the system.

\texttt{dynamic}: Display information of VLAN created dynamically by the system.

Description

Using \texttt{display vlan} command, you can view related information about the specified or all VLANs.

If \texttt{vlan\_id} or \texttt{all} is specified, information of specified VLAN or all VLANs is displayed. It includes: VLAN ID, VLAN state, whether the routing function has been enable on this VLAN (i.e. whether the route interface exists. If it exists, display IP address and mask), VLAN description, and the ports VLAN contains.

If parameter is not specified, information of the VLAN that has been created and information of whether VLAN feature has been enabled are displayed. If the parameter dynamic or static is selected, information of VLAN created dynamically or statically by the system and information of whether VLAN feature has been enabled are displayed.

For the related command, see \texttt{vlan}.

Example

\# Display the information about VLAN1.

[Quidway] display vlan 1
VLAN ID: 1
VLAN Type: static
Route interface: not configured
Description: HUAWEI
Tagged Ports: none
Untagged Ports:
  Ethernet0/1  Ethernet0/2  Ethernet0/3
1.1.3 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 interface type, interface_num is interface number and interface_name is interface name. For their meanings and value range, read 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>: Representing the repeatable times of parameters, 1 is the minimal and 10 is the maximal.

Description

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

Note that you can add/delete trunk port and hybrid port to/from 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 Ethernet0/4 through Ethernet0/7, Ethernet0/9 and Ethernet0/11 through Ethernet0/15 to VLAN 2. The repeated time of command parameter is 3 times.
    [Quidway-vlan2] port ethernet0/4 to ethernet0/7 ethernet0/9 ethernet0/11 to ethernet0/15

1.1.4 vlan

Syntax

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

View

System view

Parameter

vlan_id: Specifies the ID of a VLAN to be created and/or entered, ranging from 1 to 4094.

all: Delete all VLANs.

Description

Using vlan command, you can enter VLAN view. If the specified VLAN is not created, create it first. Using undo vlan command, you can cancel the specified VLAN.

VLAN 1 is default VLAN and cannot be deleted.

For the related commands, see display vlan.

Example

# Enter the view of VLAN 1.
[Quidway] vlan 1
[Quidway-vlan1]

1.1.5 vlan { enable | disable }

Syntax

vlan { enable | disable }

View

System view

Parameter

enable: Enable VLAN features of equipment.

disable: Disable the VLAN features of equipment.

Description

Using vlan { enable | disable } command, you can enable/disable the VLAN features of equipment.
After the VLAN is disabled, the switch will not use VLAN ID during the packet exchange, thereby losing the isolation function of VLAN domain.

For the related commands, see `display vlan`.

**Example**

# Enable the VLAN features of equipment.

[Quidway] vlan enable
Chapter 2 Isolate-User-Vlan Configuration Commands

2.1 isolate-user-vlan Configuration Commands

2.1.1 display isolate-user-vlan

Syntax

display isolate-user-vlan [ isolate-user-vlan_num ]

View

Any view

Parameter

isolate-user-vlan_num: VLAN ID of isolate-user-vlan, ranging from 1 to 4094.

Description

Using display isolate-user-vlan command, you can view the mapping relationship and the ports identifying the mapping relationship between isolate-user-vlan and Secondary VLAN.

For the related command, see isolate-user-vlan enable, isolate-user-vlan.

Example

# Display the mapping relationship between isolate-user-vlan and Secondary VLAN.

[Quidway] display isolate-user-vlan
Isolate-user-VLAN  Vlan ID : 3
Secondary Vlan ID : 4-5

Vlan ID: 3
Vlan Type: static
Isolate-user-VLAN Type : Isolate-user-VLAN
Route Interface: not configured
Description: VLAN 0003
Tagged Ports: none
Untagged Ports:
  Ethernet0/4   Ethernet0/8   Ethernet0/18

Vlan ID: 4
Vlan Type: static
Private-vlan Type: Secondary
Route Interface: not configured
Description: VLAN 0004
Tagged Ports: none
Untagged Ports:

  Ethernet0/4   Ethernet0/8

Vlan ID: 5
Vlan Type: static
Private-vlan Type: Secondary
Route Interface: not configured
Description: VLAN 0005
Tagged Ports: none
Untagged Ports:

  Ethernet0/4   Ethernet0/18

2.1.2 isolate-user-vlan

Syntax

isolate-user-vlan  isolate-user-vlan_num  secondary  secondary_vlan_numlist \[ to secondary_vlan_numlist \]

undo isolate-user-vlan  isolate-user-vlan_num \[ secondary  secondary_vlan_numlist \] \[ to secondary_vlan_numlist \]

View

System view

Parameter

isolate-user-vlan_num: VLAN ID of isolate-user-vlan, ranging from 1 to 4094.
secondary_vlan_numlist: VLAN ID of Secondary vlan, ranging from 1 to 4094.
Description

Using `isolate-user-vlan` command, you can associate isolate-user-vlan to Secondary VLAN and establish the mapping relationship between isolate-user-vlan and Secondary VLAN. Using `undo isolate-user-vlan` command, you can cancel the mapping relationship between isolate-user-vlan and Secondary VLAN.

By default, there is no any corresponding relationship between isolate-user-vlan and Secondary VLAN created by the user.

Before the command is run, isolate-user-vlan and Secondary VLAN must include ports. After the command is run, the mapping relationship between isolate-user-vlan and Secondary VLAN is established. The actual operation include: add the ports of isolate-user-vlan to every Secondary VLAN and add the ports of all Secondary VLANs to isolate-user-vlan.

After `undo` command is run, the mapping relationship between isolate-user-vlan and Secondary VLAN will be canceled. The actual operation include: delete the ports included in isolate-user-vlan from Secondary VLAN and delete the ports included in Secondary VLAN from isolate-user-vlan.

For the related command, see `display isolate-user-vlan`.

Example

```
# Associate isolate-user-vlan 10 with Secondary VLAN2, 3, 4, 5 and 9.
[Quidway] isolate-user-vlan 10 secondary 2 to 5 9
```

### 2.1.3 isolate-user-vlan enable

**Syntax**

```
isolate-user-vlan enable
undo isolate-user-vlan enable
```

**View**

VLAN view

**Parameter**

none
Description

Using **isolate-user-vlan enable** command, you can configure the type of one VLAN as isolate-user-vlan. Using **undo isolate-user-vlan enable** command, you can cancel the isolate-user-vlan type of one VLAN.

By default, the type of the VLAN created by the user has not been specified.

isolate-user-vlan can contain many ports, including the uplink ports connected to other switches. isolate-user-vlan and Trunk ports cannot be configured simultaneously, i.e., if isolate-user-vlan is configured to the Ethernet switch, the Trunk port cannot be configured. If the Trunk port is configured, then the isolate-user-vlan cannot be configured.

For the related commands, see **display isolate-user-vlan**.

Example

```bash
# Configure VLAN 5 as isolate-user-vlan.
[Quidway-vlan5] isolate-user-vlan enable
```

### 2.1.4 isolate-user-vlan igsp enable

**Syntax**

```plaintext
isolate-user-vlan igsp enable
undo isolate-user-vlan igsp enable
```

**View**

VLAN view

**Parameter**

**igsp**: Enable IGSP (IGMP Snooping Protocol).

**Description**

Use the **isolate-user-vlan igsp** command to cause IGMP packets to be sent to the route interface with Secondary VLAN IDs.

Use the **undo isolate-user-vlan igsp** command to restore the default VLAN ID of IGMP packets to be sent to the route interface.

By default, IGMP packets are sent with isolate-user-vlan ID.
Example

# Causes IGMP packets to be sent with Secondary VLAN IDs in VLAN5.

[Quidway-vlan5] isolate-user-vlan igsp enable
Chapter 3  GARP/GVRP Configuration Commands

3.1  GARP Configuration Commands

3.1.1  display garp statistics

Syntax

display garp statistics [ interface interface_list ]

View

Any view

Parameter

interface_list: List of Ethernet port to be displayed, expressed as interface_list = 
{ [ interface_type interface_num | interface_name ] [ to { interface_type interface_num |
| interface_name } ] }&<1-10>. interface_type is interface type, interface_numis
interface number and interface_name is interface name. For their meanings and value
range, read command parameters description of “Port” in this document.

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

Description

Using display garp statistics command, you can view the GARP statistics
information, including the number of received/sent packet and the number of
discarded packet by GVRP/GMRP etc.

Example

# Display the GARP statistics information on Ethernet port Ethernet0/1.

<Quidway> display garp statistics interface ethernet0/1
GARP statistics on port Ethernet0/1
   Number Of GMRP Frames Received : 0
   Number Of GVRP Frames Received : 0
   Number Of GMRP Frames Transmitted : 0
   Number Of GVRP Frames Transmitted : 0
The above information indicates that the numbers of GVRP/GMRP packets received/sent and discarded on Ethernet0/1 are 0.

3.1.2 display garp timer

Syntax

display garp timer [ interface interface_list ]

View

Any view

Parameter

interface_list: List of Ethernet port to be displayed, expressed as interface_list = 
{ { interface_type interface_num | interface_name } [ to { interface_type interface_num |
interface_name } ] }&<1-10>. interface_type is interface type, interface_num is interface number and interface_name is interface name. For their meanings and value range, read command parameters description of "Port" in this document.

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

Description

Using display garp timer command, you can view the value of GARP timer, including Hold timer, Join timer, Leave timer and LeaveAll timer.

For the related command, see garp timer, garp timer leaveall.

Example

# Show GARP timer on Ethernet0/1.

<Quidway> display garp timer interface ethernet0/1

GARP timers on port Ethernet0/1
    GARP JoinTime : 20 centiseconds
    GARP Leave Time : 60 centiseconds
    GARP LeaveAll Time : 1000 centiseconds
    GARP Hold Time : 10 centiseconds
### 3.1.3 `garp timer`

**Syntax**

```
garp timer { hold | join | leave } timer_value
undo garp timer { hold | join | leave }
```

**View**

Ethernet port view

**Parameter**

- **hold**: GARP Hold timer. After received certain registration information, the GARP application entity will not send Join Message at once, instead, it starts the Hold timer. All the registration information received within duration of the Hold timer will be transmitted in the same frame after the Hold timer times out, thereby saving the bandwidth resource.

- **join**: GARP Join timer. GARP application entity will send out Join message after the Join timer goes timeout to make other GARP application entity register its own information.

- **leave**: GARP Leave timer. When a GARP application entity wants to deregister certain attribute information, it sends Leave message. The GARP application entity received the message will starts Leave timer. If the entity receives no Join message before the timer goes timeout, it will deregister the attribute information.

- **timer_value**: Value of GARP hold timer, join timer and leave timer in centisecond. The step is 5 centiseconds. The range is according to the following rule: the value of Join timer should be no less than the doubled value of Hold timer, and the value of Leave timer should be greater than the doubled value of Join timer and smaller than the Leaveall timer value, and the minimal value of Join timer is 10 centiseconds. By default, Hold timer is 10 centiseconds, Join timer is 20 centiseconds, Leave timer is 60 centiseconds.

**Description**

Using `garp timer` command, you can configure GARP timer value. Using `undo garp timer` command, you can restore the default value of GARP timer.

For the related command, see `display garp timer`.

**Example**

```
# Set Join timer of GARP as 300ms.
```

---

Huawei Technologies Proprietary

3-3
3.1.4 garp timer leaveall

Syntax

```
garp timer leaveall timer_value
undo garp timer leaveall
```

View

System view

Parameter

```
timer_value: Value of GARP leaveall timer in centisecond, ranging from 65 to 32765. The step is 5 centiseconds. The value of Leaveall timer should be greater than the value of Leave timer. By default, the value of LeaveAll timer is 1000 centiseconds, i.e. 10s.
```

Description

Using `garp timer leaveall` command, you can configure GARP leaveall timer. Using `undo garp timer leaveall` command, you can restore the default value.

After every GARP application entity is started, the LeaveAll timer will be started simultaneously. The GARP application entity will send LeaveAll message after the timer times out to make other application entities re-register all attribute information on themselves. Then, the LeaveAll timer is started and the new cycle begins.

For the related command, see `display garp timer`.

Example

```
# Set GARP LeaveAll timer as 1s.
[Quidway] garp timer leaveall 100
```

3.1.5 reset garp statistics

Syntax

```
reset garp statistics [ interface interface_list ]
```

View

User view

Parameter

\textit{interface\_list}: Specifies a list of Ethernet ports, on which the GARP statistics information will be cleared, expressed as \textit{interface\_list} = \{ \{ \textit{interface\_type} \textit{interface\_num} \mid \textit{interface\_name} \} [ to \{ \textit{interface\_type} \textit{interface\_num} \mid \textit{interface\_name} \} ] \} &<1-10>. \textit{interface\_type} is interface type, \textit{interface\_num} is interface number and \textit{interface\_name} is interface name. For their meanings and value range, read Parameter Description of “Port” in this document.

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

Description

Using \texttt{reset garp statistics} command, you can reset the GARP statistics information (such as the received/sent packets or discarded packets by GVRP/GMRP). If the command has no parameter, it will clear the GARP statistics information of all the ports.

For the related command, see \texttt{display garp statistics}.

Example

\begin{verbatim}
# Clear GARP statistics information.
<Quidway> reset garp statistics
\end{verbatim}

\section*{3.2 GVRP Configuration Command}

\subsection*{3.2.1 display gvrp statistics}

Syntax

\texttt{display gvrp statistics [ interface interface\_list ]}

View

Any view
Parameter

interface_list: List of Ethernet port to be displayed, expressed as interface_list = {{ interface_type interface_num | interface_name } \to { interface_type interface_num | interface_name } } \&<1-10>. interface_type is interface type, interface_num is interface number and interface_name is interface name. For their meanings and value range, read command parameters description of “Port” in this document.

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

Description

Using display gvrp statistics command, you can view the GVRP statistics information of all the Trunk ports, including the list of ports enabled with GVRP, GVRP status information, failed GVRP registration entries and the last GVRP data unit origin etc.

Example

# Display the GVRP statistics information about Ethernet0/1.

<Quidway> display gvrp statistics interface ethernet0/1

GVRP statistics on port Ethernet0/1

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

3.2.2 display gvrp status

Syntax

display gvrp status

View

Any view

Parameter

none
Description

Using `display gvrp status` command, you can view the global status information about GVRP.

Example

# Display the global status information about GVRP.

<Quidway> display gvrp status
    GVRP is enabled

3.2.3 gvrp

Syntax

```
gvrp
undo gvrp
```

View

System view/Ethernet port view

Parameter

none

Description

Using `gvrp` command, you can enable GVRP. Using `undo gvrp` command, you can restore the GVRP to default mode, i.e. disable GVRP.

By default, GVRP is disabled.

This command can be used to enable/disable global GVRP in System view or enable/disable port GVRP in Ethernet port view.

Before enabling port GVRP, the user must enable global GVRP first and port GVRP must be enabled/disabled on Trunk port.

For the related commands, see `display gvrp status`.

Example

# Enable global GVRP.

[Quidway] gvrp
3.2.4  gvrp registration

Syntax

    gvrp registration { fixed | forbidden | normal }
    undo gvrp registration

View

    Ethernet port view

Parameter

    fixed: Enable to create or register VLAN on the port manually and disable to register or deregister VLAN dynamically.

    forbidden: Deregisters all VLANs except VLAN 1 and disables to create or register any other VLAN on the port.

    normal: Enable to create, register and deregister VLAN on the port manually or dynamically.

Description

    Using gvrp registration command, you can configure GVRP registration type. Using undo gvrp registration command, you can restore the default type.

    By default, the registration type is normal.

    This command can be only used on Trunk port.

    For the related commands, see display gvrp statistics.

Example

    # Set the GVRP registration type of Ethernet0/1 as fixed.
    [Quidway-Ethernet0/1] gvrp registration fixed
Chapter 4 Voice VLAN Configuration Commands

4.1 Voice VLAN Configuration Commands

4.1.1 display voice vlan oui

Syntax

display voice vlan oui

View

Any view

Parameter

None

Description

Using the display voice vlan oui command, you can display the OUI address supported by the current system and its relative features.

For related commands, see voice vlan vlan_id enable and voice vlan enable.

Example

# Display the OUI address of Voice VLAN.
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] display voice vlan oui

<table>
<thead>
<tr>
<th>Oui Address</th>
<th>Mask</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00e0-bb00-0000</td>
<td>ffff-ff00-0000</td>
<td>3com phone</td>
</tr>
<tr>
<td>0003-6b00-0000</td>
<td>ffff-ff00-0000</td>
<td>Cisco phone</td>
</tr>
<tr>
<td>00e0-7500-0000</td>
<td>ffff-ff00-0000</td>
<td>Polycom phone</td>
</tr>
<tr>
<td>00d0-1e00-0000</td>
<td>ffff-ff00-0000</td>
<td>Pingtel phone</td>
</tr>
<tr>
<td>00aa-bb00-0000</td>
<td>ffff-ff00-0000</td>
<td>ABC</td>
</tr>
</tbody>
</table>
4.1.2 display voice vlan status

Syntax

display voice vlan status

View

Any view

Parameter

None

Description

Using the **display voice vlan status** command, you can display the relative Voice VLAN features including the Voice VLAN status, the configuration mode, and the current Voice VLAN port status, and so on.

For related commands, see **voice vlan vlan_id enable** and **voice vlan enable**.

Example

# Enable the Voice VLAN on VLAN 2 and display the Voice VLAN status.

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] display voice vlan status
Voice Vlan status: ENABLE
Voice Vlan ID: 2
Voice Vlan security mode: Security
Voice Vlan aging time: 100 minutes
Current voice vlan enabled port mode:
PORT          MODE
-------------------------
Ethernet0/12    AUTO
Ethernet0/13    MANUAL
```

4.1.3 voice vlan aging

Syntax

voice vlan aging minutes

undo voice vlan aging
View

System view

Parameter

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

Description

Using the voice vlan aging command, you can set the aging time of Voice VLAN. Using the undo voice vlan aging command, you can set the aging time back to the default.

For the related command, see display voice vlan status.

Example

# Set the aging time of Voice VLAN to 100 minutes.
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] voice vlan aging 100
[Quidway]

4.1.4 voice vlan enable

Syntax

voice vlan enable

undo voice vlan enable

View

Ethernet Port view

Parameter

None

Description

Using the voice vlan enable command, you can enable the Voice VLAN features on the port. Using the undo voice vlan enable command, you can disable its Voice VLAN features.
Only the Voice VLAN features in system view and port view are all enabled can the Voice VLAN function on the port run normally.

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

**Example**

```
# Enable the Voice VLAN features on port Ethernet1/0/2.
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] interface ethernet1/0/2
[Quidway-Ethernet1/0/2] voice vlan enable
```

### 4.1.5 voice vlan

**Syntax**

```plaintext
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**

Using the `voice vlan` command, you can globally enable the Voice VLAN features of one VLAN. Using the `undo voice vlan enable` command, you can globally disable its Voice VLAN features.

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. Only one VLAN can enable Voice VLAN at one time.

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

**Example**

```
# Enable the Voice VLAN features on VLAN 2.
<Quidway> system-view
```
System View: return to User View with Ctrl+Z.

[Quidway] vlan 2
[Quidway-vlan2] quit
[Quidway] voice vlan 2 enable

# Enable the Voice VLAN features on VLAN 2

# If you enable the Voice VLAN features on other VLAN while the Voice VLAN features on VLAN 2 has been enabled, the configuration fails.

[Quidway] voice vlan 4 enable
Can't change voice vlan configuration when other voice vlan is running

4.1.6 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 of H-H-H.
- **oui-mask**: The valid length of a MAC address, represented by a mask, and in the format of H-H-H.
- **string**: Description of the MAC address, in the range of 1 to 30.

Description

Using the `voice vlan mac-address` command, you can set the MAC address that the Voice VLAN can control. Using the `undo voice vlan mac-address` command, you can cancel this MAC address.

Here the OUI address refers to a vendor’s 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 4-1** Default OUI addresses

<table>
<thead>
<tr>
<th>No.</th>
<th>OUI</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00e0-bb00-0000</td>
<td>3com phone</td>
</tr>
</tbody>
</table>
For the related command, see `display voice vlan oui`.

**Example**

```
# Set the MAC address 00AA-BB00-0000 as an OUI address.

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

### 4.1.7 voice vlan mode

**Syntax**

```
voice vlan mode auto
undo voice vlan mode auto
```

**View**

Ethernet port view

**Parameter**

None

**Description**

Using the `voice vlan mode auto` command, you can set the Voice VLAN in auto mode. Using the `undo voice vlan mode auto` command, you can set the Voice VLAN in manual mode.

By default, the Voice VLAN is in auto mode.

If needed, 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`.

<table>
<thead>
<tr>
<th></th>
<th>OUI Address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0003-6b00-0000</td>
<td>Cisco phone</td>
</tr>
<tr>
<td>3</td>
<td>00e0-7500-0000</td>
<td>Polycom phone</td>
</tr>
<tr>
<td>4</td>
<td>00d0-1e00-0000</td>
<td>Pingtel phone</td>
</tr>
</tbody>
</table>
Example

# Set the Voice VLAN in manual mode.

```
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] interface Ethernet0/13
[Quidway-Ethernet0/13] undo voice vlan mode auto
```

4.1.8 voice vlan security enable

**Syntax**

```
voice vlan security enable
undo voice vlan security enable
```

**View**

System view

**Parameter**

None

**Description**

Using the `voice vlan security enable` command you can 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. Using the `undo voice vlan security enable` command, you can 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**

# Disable the Voice VLAN security mode.

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

## Chapter 1 GMRP Configuration Commands
1.1 GMRP Configuration Commands ...................................................... 1-1
   1.1.1 debugging gmrp ................................................................. 1-1
   1.1.2 display gmrp statistics ..................................................... 1-1
   1.1.3 display gmrp status .......................................................... 1-2
   1.1.4 gmrp ................................................................................. 1-3

## Chapter 2 IGMP Snooping Configuration Commands
2.1 IGMP Snooping Configuration Commands .................................. 2-1
   2.1.1 display igmp-snooping configuration .................................. 2-1
   2.1.2 display igmp-snooping group .......................................... 2-2
   2.1.3 display igmp-snooping statistics ..................................... 2-3
   2.1.4 display multicast-source-deny ......................................... 2-3
   2.1.5 igmp-snooping ................................................................. 2-4
   2.1.6 igmp-snooping fast-leave ................................................. 2-5
   2.1.7 igmp-snooping group-limit ............................................ 2-5
   2.1.8 igmp-snooping group-policy .......................................... 2-6
   2.1.9 igmp-snooping host-aging-time ...................................... 2-8
   2.1.10 igmp-snooping max-response-time ............................... 2-8
   2.1.11 igmp-snooping router-aging-time .................................. 2-9
   2.1.12 multicast-source-deny .................................................. 2-10
   2.1.13 reset igmp-snooping statistics ......................................... 2-11

## Chapter 3 Unknown Multicast Dropping Configuration Commands
3.1 Unknown Multicast Dropping Configuration Commands ........... 3-1
   3.1.1 unknown-multicast drop enable ...................................... 3-1

## Chapter 4 Multicast MAC Address Configuration Commands
4.1 Multicast MAC Address Configuration Commands .................. 4-1
   4.1.1 mac-address multicast .................................................. 4-1

## Chapter 5 Multicast VLAN Configuration Commands
5.1 Multicast VLAN Configuration Commands ............................... 5-1
   5.1.1 service-type multicast .................................................. 5-1
Chapter 1  GMRP Configuration Commands

1.1  GMRP Configuration Commands

1.1.1  debugging gmrp

Syntax

    debugging gmrp { event | packet }
    undo debugging gmrp { event | packet }

View

    User view

Parameter

    event: GMRP event.
    packet: GMRP packet.

Description

    Using debugging gmrp command, you can enable GMRP debugging. Using undo debugging gmrp you can disable GMRP debugging.

Example

    # Enable GMRP event debugging.
    <Quidway> debugging gmrp event
    GMRP: Max number of GMRP entries reached

    Table 1-1 Description of information generated by the command debugging gmrp event

    | Field                                | Description                                      |
    |--------------------------------------|--------------------------------------------------|
    | GMRP: Max number of GMRP entries reached | Maximum number of entries reached for GMRP local database |

1.1.2  display gmrp statistics

Syntax

    display gmrp statistics [ interface interface-list ]
View

Any view

Parameter

interface interface-list: Specifies Ethernet port list, expressed as interface-list = { { interface_type interface_num | interface_name } [ to { interface_type interface_num | interface_name } ] }&<1-10>. For meanings and value ranges of interface-type, interface-number and interface-name, refer to the syntax description in the Port Configuration of this manual.

Description

Using display gmrp statistics command, you can view the statistics information about GMRP.

This command is used for displaying the statistics information about GMRP, including the list of ports with GMRP enabled, GMRP status information, GMRP failed registrations and last origin of GMRP packet data unit (PDU).

Example

# Display the statistics information about GMRP on Ethernet 0/1.
<Quidway> display gmrp statistics interface Ethernet 0/1
GMRP statistics on port Ethernet0/1
Gmrp Status : Enabled
Gmrp Failed Registrations : 0
Gmrp Last Pdu Origin : 0000-0000-0000

1.1.3 display gmrp status

Syntax

display gmrp status

View

Any view

Parameter

None

Description

Using display gmrp status command, you can view the status of global GMRP.

This command can be used for displaying the enabled/disabled status of global GMRP.

Huawei Technologies Proprietary


Example

# Display the status of global GMRP.
<Quidway> display gmrp status
GMRP is enabled

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GMRP is enabled</td>
<td>GMRP is enabled globally.</td>
</tr>
</tbody>
</table>

1.1.4 gmrp

Syntax

```
gmrp
undo gmrp
```

View

System view/Ethernet port view

Parameter

None

Description

Using `gmrp` command, you can enable global GMRP or enable GMRP on a port. Using `undo gmrp` command, you can configure the GMRP back to the default setting, namely disabled.

By default, GMRP is disabled

Executed in system view, this command will enable the global GMRP. After performing this command in Ethernet port view, GMRP will be enabled on a port.

Before enabling GMRP on a port, you shall enable GMRP globally.

For the related command, see `display gmrp status, display gmrp statistics`.

Example

# Enable GMRP globally.
[Quidway] gmrp
Chapter 2  IGMP Snooping Configuration Commands

2.1  IGMP Snooping Configuration Commands

2.1.1  display igmp-snooping configuration

Syntax

display igmp-snooping configuration

View

Any view

Parameter

None

Description

Using display igmp-snooping configuration command, you can 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.

For the related command, see igmp-snooping.

Example

# Display the IGMP Snooping configuration information of the switch.
<Quidway> 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.
2.1.2  display igmp-snooping group

Syntax

display igmp-snooping group [ vlan vlanid ]

View

Any view

Parameter

vlan vlanid: 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

Using display igmp-snooping group command, you can 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.

<Quidway> display igmp-snooping group vlan 2
***************Multicast group table***************
Vlan(id):2.
Router port(s):Ethernet0/1
IP group(s):the following ip group(s) match to one mac group.
IP group address:230.45.45.1
Member port(s):Ethernet0/12
MAC group(s):
MAC group address:01-00-5e-2d-2d-01
Member port(s):Ethernet0/12

We can know from the information listed above that:

- There is a multicast group in VLAN 2;
- The router port is Ethernet 0/1;
- The address of the multicast group is 230.45.45.1;
- The member of the IP multicast group is Ethernet 0/12;
- MAC multicast group is 0100-5e2d-2d01;
- The member of the MAC multicast group is Ethernet 0/12.
2.1.3 display igmp-snooping statistics

Syntax

display igmp-snooping statistics

View

Any view

Parameter

None

Description

Using display igmp-snooping statistics command, you can view the statistics information on IGMP Snooping.

This command displays the statistics information about IGMP Snooping of 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.

For the related command, see igmp-snooping.

Example

# Display statistics information about IGMP Snooping.
<Quidway> 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.

2.1.4 display multicast-source-deny

Syntax

display multicast-source-deny [ interface { interface_type [ interface_number ] | interface_name } ]

View

Any view
Parameter

\[ \text{interface}_\text{type} \]: Port type.
\[ \text{interface}_\text{number} \]: Interface number.
\[ \text{interface}_\text{name} \]: Interface name, expressed as \( \text{interface}_\text{name} = \text{interface}_\text{type} \times \text{interface}_\text{number} \).

Description

Use the `display multicast-source-deny` command to display configuration information about multicast source port checking.

If the port type and port number are not specified, the multicast source port checking information about all ports on the switch is displayed; if only the port type is specified, the multicast source port checking information about all ports of this type is displayed; if both the port type and port number are specified, then the multicast source port checking information about this port is displayed.

Example

# Display the state of multicast source port suppression on ethernet 0/1.
[Quidway] display multicast-source-deny ethernet 0/1

# Display the state of multicast source port suppression on all 100 Mbps Ethernet ports.
[Quidway] display multicast-source-deny interface ethernet

2.1.5 igmp-snooping

Syntax

\[ \text{igmp-snooping} \{ \text{enable} | \text{disable} \} \]
\[ \text{undo igmp-snooping} \]

View

System view

Parameter

\[ \text{enable} \]: Enable IGMP Snooping.
\[ \text{disable} \]: Disables IGMP Snooping; By default, the switch disables IGMP Snooping feature.

Description

Using `igmp-snooping` command, you can enable/disable IGMP Snooping. Using `undo igmp-snooping` command, you can restore the default setting.

This command is used to enable or disable IGMP Snooping on the switch.
Example

# Enable IGMP Snooping.
[Quidway] igmp-snooping enable

2.1.6 igmp-snooping fast-leave

Syntax

igmp-snooping fast-leave
undo igmp-snooping fast-leave

View

Ethernet port view

Parameter

None

Description

Using the `igmp-snooping fast-leave` command, you can enable the function of fast removing a port from a multicast group. Using the `undo igmp-snooping fast-leave` command, you can cancel this configuration.

By default, the fast remove function is disabled.

Normally, at the receiving of the IGMP Leave packet, `igmp-snooping` sends out group-specific query packet instead of directly removing a port from a multicast group. After waiting for a period of time, if it receives no respond, `igmp-snooping` then removes the port from the group. By configuring this command, `igmp-snooping` removes the port from the multicast group directly at receiving the IGMP Leave packet. The fast remove function saves bandwidth when only one user remaining at the port.

Note that, this function takes effect on condition that the client supports IGMP V2. After configuring this command, when there are multiple users at one port, the leaving of one user may cause the loss of multicast service of other users in this group.

Example

# Enable the the fast remove function on Ethernet 0/1.
[Quidway-Ethernet0/1] igmp-snooping fast-leave

2.1.7 igmp-snooping group-limit

Syntax

igmp-snooping group-limit `limit`
undo igmp-snooping group-limit
View

Ethernet port view

Parameter

\textit{limit}: The maximum number of multicast groups on a port, in the range of 0 to 1000. The default value is 1000.

Description

Using \texttt{igmp-snooping group-limit} command, you can set the maximum number of multicast groups permitted on a port. Using \texttt{undo igmp-snooping group-limit} command, you can restore the default value.

By default, the maximum number of multicast groups permitted on a port is unlimited.

Example

\begin{verbatim}
# Set the maximum number of multicast groups permitted on Ethernet0/1 is 200.
[Quidway-Ethernet0/1] igmp-snooping group-limit 200
\end{verbatim}

2.1.8 \texttt{igmp-snooping group-policy}

Syntax

\texttt{igmp-snooping group-policy acl\_number vlan \textit{vlan}\_id}

\texttt{undo igmp-snooping group-policy vlan \textit{vlan}\_id}

View

Ethernet port view

Parameter

\texttt{acl\_number}: Number of basic access control list, in the range of 2000 to 2999.

\texttt{vlan\_id}: ID of VLAN to which the ethernet port belongs, ranging from 1 to 4094.

Description

Using \texttt{igmp-snooping group-policy} command, you can set the filtering of IGMP Snooping to control the accessing to the multicast group. Using \texttt{undo igmp-snooping group-policy} command, you can cancel the configured filtering.

By default, no filtering is configured on the switch.

IGMP snooping filter function can limit the programs that users can order, by configuring some multicast filtering ACLs for users on the different switch ports, so that different users can order different program sets.

In practice, when ordering a multicast program set, the user originates an IGMP report packet. Upon receiving the packet, the switch first compares it against the multicast
ACLs configured on the inbound port. If allowed, the switch then adds the port to the forward port list of the multicast group; otherwise, it drops the IGMP report packet and no data flow then will be sent to this port. Thus the switch can control users’ multicast program ordering.

User-defined ACL rule is a multicast address or multicast address range (224.0.0.1 to 239.255.255.255)
- If the rule is set as permit, the port can be added to the groups contained in the permitted ACL range, but not to the groups outside the permitted ACL range.
- If the rule is set as deny and no other ACL is set as permit, the port cannot be added to the groups within the denied ACL range, nor to the groups outside the denied ACL range.

**Note:**
- Each VLAN of each port can only be configured with one ACL rule.
- If no ACL rule is configured or the configured port doesn’t belong to the specified VLAN, the filtering configured by this command will not take effect.
- Most devices just broadcast unknown multicast packets, so to prevent the case where multicast data flow is sent as unknown multicast packets to the filtered ports, this function is generally configured in combination with the unknown multicast dropping function.

For the related command, see `unknown-multicast drop enable`.

**Example**

```bash
# Configure ACL 2000 to permit the accessing to multicast group 225.0.0.0~225.255.255.255.
[Quidway-acl-basic-2000] rule permit source 225.0.0.0 0.255.255.255

# Create VLAN 2, and add Ethernet 0/1 to it.
[Quidway-vlan2] port Ethernet 0/1

# Set the filtering of IGMP Snooping Report packets applied to ACL 2000 of VLAN 2 on Ethernet 0/1.
[Quidway] interface Ethernet 0/1
[Quidway-Ethernet0/1] igmp-snooping group-policy 2000 vlan 2

# Configure ACL 2001 to deny the accessing to multicast group 225.0.0.0~225.255.255.255 and permit the accessing outside the range.
[Quidway-acl-basic-2000] rule deny source 224.0.0.0 0.255.255.255
```

Create VLAN 2, and add Ethernet 0/2 to it.

```
[Quidway] vlan 2
[Quidway-vlan2] port Ethernet 0/2
```

Set the filtering of IGMP Snooping Report packets applied to ACL 2001 of VLAN 2 on Ethernet 0/2.

```
[Quidway] interface Ethernet 0/2
[Quidway-Ethernet0/2] igmp-snooping group-policy 2001 vlan 2
```

### 2.1.9 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; By default, 260.

**Description**

Using `igmp-snooping host-aging-time` command, you can configure the port aging time of the multicast group members. Using `undo igmp-snooping host-aging-time` command, you can restore the default value.

This command is used to set 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.

For the related command, see `igmp-snooping`.

**Example**

```
# Set the aging time to 300 seconds.
[Quidway] igmp-snooping host-aging-time 300
```

### 2.1.10 igmp-snooping max-response-time

**Syntax**

```
igmp-snooping max-response-time seconds
```

---

Huawei Technologies Proprietary

2-8
undo igmp-snooping max-response-time

View

System view

Parameter

seconds: Maximum response time for a query ranging from 1 to 100 and measured in seconds; By default, 10.

Description

Using `igmp-snooping max-response-time` command, you can configure the maximum response time for a query. Using `undo igmp-snooping max-response-time` command, you can restore the default value.

The set maximum response time decides the time limit for the switch to respond to IGMP Snooping general query packets.

For the related command, see `igmp-snooping`, `igmp-snooping router-aging-time`.

Example

# Configure to respond the IGMP Snooping packet within 50s.
[Quidway] igmp-snooping max-response-time 50

2.1.11  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 130 to 1000 measured in seconds; By default, 260.

Description

Using `igmp-snooping router-aging-time` command, you can configure the router port aging time of IGMP Snooping. Using `undo igmp-snooping router-aging-time` command, you can restore the default value.

The port here refers to the Ethernet 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.
For the related command, see `igmp-snooping`, `igmp-snooping max-response-time`.

**Example**

```plaintext
# Set the aging time of the IGMP Snooping router port to 500 seconds.
[Quidway] igmp-snooping router-aging-time 500
```

### 2.1.12 multicast-source-deny

**Syntax**

```plaintext
multicast-source-deny [ interface interface-list ]
undo multicast-source-deny [ interface interface-list ]
```

**View**

System view or Ethernet port view

**Parameter**

`interface interface-list`: Ethernet port list, indicates multiple Ethernet ports, in the format of `interface-list = { interface-num [ to interface-num ] } & < 1-10 >`, where `interface-num` is a single Ethernet port and can be expressed as `interface-num = { interface-type interface-num | interface-name }; interface-num` is port number, and `interface-name` is the port name, see the command parameters in the *Port Configuration* section of this manual for their meanings and value ranges.

**Description**

Use the `multicast-source-deny` command to enable the multicast source port suppression function.

Use the `undo multicast-source-deny` command to return to the defaults.

By default, the multicast source port suppression function is disabled on all ports.

This feature is to filter multicast packets on an unauthorized multicast source port, preventing the user that connects to this port from setting multicast server privately.

In system view, if the `interface-list` parameter is not specified, it means that to enable this function globally; if the `interface-list` parameter is specified, it means that to enable it on the specified port. In Ethernet port view, the `interface-list` parameter cannot be specified, and you can use this command only to enable the feature on the current port.

**Example**

```plaintext
# Enable multicast source port suppression on all ports of the switch
[Quidway] multicast-source-deny
```
# Enable multicast source port suppression on ports ethernet 0/1 to ethernet 0/10, and ethernet 0/12.

```bash
[Quidway] multicast-source-deny interface ethernet 0/1 to ethernet 0/10 ethernet 0/12
```

## 2.1.13 `reset igmp-snooping statistics`

### Syntax

```
reset igmp-snooping statistics
```

### View

User view

### Parameter

None

### Description

Using `reset igmp-snooping statistics` command, you can reset the IGMP Snooping statistics information.

For the related command, see `igmp-snooping`.

### Example

```bash
# Clear IGMP Snooping statistics information.
<Quidway> reset igmp-snooping statistics
```
Chapter 3 Unknown Multicast Dropping
Configuration Commands

3.1 Unknown Multicast Dropping Configuration Commands

3.1.1 unknown-multicast drop enable

Syntax

unknown-multicast drop enable
undo unknown-multicast drop enable

View

System view

Parameter

None

Description

Using **unknown-multicast drop enable** command, you can enable the unknown multicast dropping function. Using **undo unknown-multicast drop enable** command, you can disable this function.

By default, the unknown multicast dropping function is disabled.

Normally, if the multicast address of multicast data packet received by the switch is not registered on this switch, this packet will be broadcasted within this VLAN. Whereas after enabling the unknown multicast dropping feature, when receiving multicast data packet with unregistered multicast address, the switch will drop this packet. In this way, the bandwidth is saved, and the efficiency of the system is enhanced.

Example

# Enable the switch to drop multicast data packets with unregistered multicast addresses.

[Quidway] unknown-multicast drop enable
Chapter 4 Multicast MAC Address Configuration

Commands

4.1 Multicast MAC Address Configuration Commands

4.1.1 mac-address multicast

Syntax

```
mac-address multicast mac-address interface interface-list vlan vlan_id
undo mac-address multicast { mac-address interface interface-list vlan vlan_id |
[ mac-address ] | [ interface interface-list ] | [ vlan vlan_id ] }
```

View

System view

Parameter

- `mac-address`: Multicast MAC address.
- `interface-list`: Forwarding port list, in format of `interface-list = { { interface-type interface-num | interface-name } | { interface-type interface-num | interface-name } | to { interface-type interface-num | interface-name } }`.
- `vlan_id`: Specifies VLAN ID.

Description

Use the `mac-address multicast` command to add multicast MAC address entries.

Use the `undo mac-address multicast` command to delete multicast MAC address entries.

A multicast entry includes multicast address, forwarding port, VLAN etc.

Related command: `display mac-address multicast`, `display mac-address multicast count`.

Example

```
# Create a multicast MAC address entry on the switch, with its multicast address as 0100-5e0a-0805, forwarding port as Ethernet 1/0/1 and it belonging to VLAN1.
<Quidway> system-view
System View: return to User View with Ctrl+Z.
```
[Quidway] mac-address multicast 0100-5e0a-0805 interface Ethernet 1/0/1 vlan 1
Chapter 5 Multicast VLAN Configuration Commands

5.1 Multicast VLAN Configuration Commands

5.1.1 service-type multicast

Syntax

service-type multicast
undo service-type multicast

View

VLAN view

Parameter

None

Description

Use the service-type multicast command to set the current VLAN to multicast VLAN. Use the undo service-type multicast command to cancel the setting.

By default, no VLAN is a multicast VLAN.

You can configure a multicast VLAN, join related switch ports into this VLAN and enable the IGMP Snooping function to make users in different VLANs share the same multicast VLAN. After doing that, multicast streams are transmitted only through the multicast VLAN, and therefore the bandwidth is saved. Additionally, the absolute isolation between the multicast VLAN and the user VLANs guarantees the security of the network.

Example

# Set VLAN 2 to multicast VLAN.
<Quidway> system-view
[Quidway] vlan 2
[Quidway-vlan2] service-type multicast
# Table of Contents

**Chapter 1 ACL Commands**

1.1 ACL Configuration Command List

1.1.1 acl

1.1.2 display acl config

1.1.3 display acl running-packet-filter all

1.1.4 display time-range

1.1.5 packet-filter

1.1.6 reset acl counter

1.1.7 rule

1.1.8 time-range

---

**Chapter 2 QoS Commands**

2.1 QoS Configuration Commands List

2.1.1 display qos cos-local-precedence-map

2.1.2 display qos-global all

2.1.3 display qos-global mirrored-to

2.1.4 display qos-global traffic-priority

2.1.5 display qos-global traffic-redirect

2.1.6 display qos-global traffic-statistic

2.1.7 display qos-interface all

2.1.8 display qos-interface line-rate

2.1.9 display qos-interface traffic-limit

2.1.10 display queue-scheduler

2.1.11 line-rate

2.1.12 mirrored-to

2.1.13 priority

2.1.14 priority trust

2.1.15 qos cos-local-precedence-map

2.1.16 queue-scheduler

2.1.17 reset traffic-statistic

2.1.18 traffic-limit

2.1.19 traffic-priority

2.1.20 traffic-redirect

2.1.21 traffic-statistic

---

**Chapter 3 Logon user’s ACL control command**

3.1 Logon user’s ACL control command

3.1.1 acl

3.1.2 ip http acl
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.3 snmp-agent community</td>
<td>3-2</td>
</tr>
<tr>
<td>3.1.4 snmp-agent group</td>
<td>3-3</td>
</tr>
<tr>
<td>3.1.5 snmp-agent usm-user</td>
<td>3-4</td>
</tr>
</tbody>
</table>
Chapter 1 ACL Commands

1.1 ACL Configuration Command List

1.1.1 acl

Syntax

```
    acl { number acl-number | name acl-name [ advanced | basic | link | user ] } 
    [ match-order { config | auto } ]
    undo acl { number acl-number | name acl-name | all }
```

View

System view

Parameter

- **number acl-number**: Access list number, ranging from:
  - 2000 to 2999: Basic ACL.
  - 3000 to 3999: Advanced ACL.
  - 4000 to 4999: L2 ACL.
  - 5000 to 5999: User-defined ACL.
- **name acl-name**: Specifies an access list with a character string, beginning with English letters [a-z, A-Z] only, excluding space and quotation marks, and not case sensitive. The all and any keywords are not allowed.
- **advanced**: Advanced ACL.
- **basic**: Basic ACL.
- **link**: L2 ACL.
- **user**: User-defined ACL.
- **config**: Follow the user configuration order to match ACL rules.
- **auto**: Follow the depth-first order to match ACL rules.
- **all**: Configures to delete all the ACLs (including numbered and named ACLs).

Description

Using **acl** command, you can configure a numbered or named ACL, and enter the corresponding ACL view. Using **undo acl** command, you can cancel all the rules of a numbered or named ACL or all the ACLs.
By default, the ACLs are matched in config order. You can use the acl command to create an ACL and specify its name with "acl-name" and its type with the keywords "advanced", "basic", "link", or "user". For both numbered and named ACL, you can use the rule command to add rules for them after entering ACL view. (Use the quit command to exit ACL view.) An ACL may contain multiple rules and the traffic classification rules concern different ranges, which brings forward the issue of match order when a data packet matches more than one rule.

Using the match-order parameter, you can configure to follow the user configuration order (as defaulted) or depth-first order (matching the rule with smaller range first) to match the rules. After specified the match order of an ACL, you cannot change it, unless delete all its rules and specify the order again. Note that, the match order of ACL can only be effective in the case ACL is cited by software to filter and classify data.

Due to the chips installed, the hardware match order of ACL's sub-rule is different in different switch models. The details are listed in the following table.

Table 1-1 Hardware match order of ACL's sub-rule

<table>
<thead>
<tr>
<th>Switch</th>
<th>Hardware match order of ACL's sub-rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>S3000-EI series</td>
<td>An ACL is configured with multiple sub-rules. The latest sub-rule will be matched first.</td>
</tr>
</tbody>
</table>

For related configurations, refer to the command rule.

Example

```bash
# Configure to follow depth-first order to match the rules of ACL 2000.
[Quidway] acl number 2000 match-order auto
```

1.1.2 display acl config

Syntax

```
display acl config { all | acl-number | acl-name }
```

View

Any view

Parameter

- **all**: Configures to display all the ACLs (including numbered and named ACLs).
- **acl-number**: Specifies the sequence number of the ACL to be displayed with a number between 2000 and 3999.
**acl-name**: Specifies the name of the ACL to be displayed with a character string starting with English letters ([a-z, A-Z]) only and excluding space or quotation mark.

**Description**

Using `display acl config` command, you can view the detail configuration information about the ACL, including all the statements and sequence numbers and how many packets and bytes matched these statements. The matched information is the information treated by switch’s CPU. The matched information of transmitted data can be displayed by `display qos-global traffic-statistic` command.

**Example**

```
# Display the content of all the ACLs.
<Quidway> display acl config all
Basic ACL 2010, 1 rule,
    rule 1 permit 10.0.0.1 0 (0 times matched)

Basic ACL 2020, 1 rule,
    rule 2 permit 20.0.0.1 0 (0 times matched)

Basic ACL std1, 2 rules,
    rule 1 permit 20.0.0.1 0 (0 times matched)
    rule 2 permit 30.0.0.1 0 (0 times matched)
```

**Table 1-2 the display Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic ACL 2010, 1 rule, rule 1 permit 10.0.0.1 0 (0 times matched)</td>
<td>“Basic ACL” delegates the type of ACL, the type of ACL can be “advanced ACL”, “Basic ACL”, “Interface based ACL” or “Link ACL”. “2010” indicates the number of ACL (in this location, it may be the name of the ACL), “1 rule” indicates the rule number of the ACL. “rule 1 permit 10.0.0.1 0 (0 times matched)” indicates the rule’s content</td>
</tr>
</tbody>
</table>

1.1.3 `display acl running-packet-filter all`

**Syntax**

`display acl running-packet-filter all`

**View**

Any view
Parameter

None

Description

Using `display acl running-packet-filter all` command, you can view the information about the running state of the ACL. The displayed information includes ACL name, rule name and running state.

Example

# Display the ACL running state on all the interfaces.
<Quidway> display acl running-packet-filter all
acl std1 rule 0  running
acl std1 rule 1  running

The display information shows all the activated ACLs of the switch.

1.1.4 display time-range

Syntax

display time-range { all | name }

View

Any view

Parameter

all: Configures to display all the time range.
name: Specifies the name of the time range.

Description

Using `display time-range` command, you can view the configuration and status of the current time range. You will see the active or inactive state outputs respectively.

Note that the system has a delay of about 1 minute when updating the ACL state, while the `display time-range` command applies the current time. Therefore when `display time-range` displays that a time range is active, the ACL using it may not have been activated. This is a kind of normal case.

Example

# Display the configuration of all the time ranges.
<Quidway> display time-range all
Current time is 14:36:36 4-3-2003 Thursday

Time-range : hhy ( Inactive )
from 08:30 2-5-2005 to 18:00 2-19-2005

Time-range : hhy1 ( Inactive )
from 08:30 2-5-2003 to 18:00 2-19-2003

Table 1-3 the display Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current time is 14:36:36 4-3-2003 Thursday</td>
<td>Indicates the current time of the switch (according to the switch setting).</td>
</tr>
<tr>
<td>Time-range: hhy ( Inactive )</td>
<td>Indicates the name of the time-range. &quot; ( Inactive ) &quot; indicates the status of this time-range is not active at current time.</td>
</tr>
<tr>
<td>from 08:30 2-5-2005 to 18:00 2-19-2005</td>
<td>The content of time-range: the first time is the beginning time, the last time is the ending time.</td>
</tr>
</tbody>
</table>

# Display the time range named tm1.
<Quidway> display time-range tm1
Current time is 14:37:31 4-3-2003 Thursday

Time-range : tm1 ( Inactive )
from 08:30 2-5-2005 to 18:00 2-19-2005

Table 1-4 the display Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current time is 14:36:36 4-3-2003 Thursday</td>
<td>Indicates the current time of the switch (according to the switch setting).</td>
</tr>
<tr>
<td>Time-range : tm1 ( Inactive )</td>
<td>Indicates the name of the time-range. &quot; ( Inactive ) &quot; indicates the status of this time-range is not active at current time.</td>
</tr>
<tr>
<td>from 08:30 2-5-2005 to 18:00 2-19-2005</td>
<td>The content of time-range: the first time is the beginning time, the last time is the ending time.</td>
</tr>
</tbody>
</table>

1.1.5 packet-filter

Syntax

```bash
class-filter { user-group { acl-number | acl-name } [ rule rule ] | ip-group { acl-number | acl-name } [ rule rule ] | link-group { acl-number | acl-name }[ rule rule ])*
```

Huawei Technologies Proprietary

1-5
undo packet-filter { user-group { acl-number | acl-name } [ rule rule ] | ip-group { acl-number | acl-name } [ rule rule ] | link-group { acl-number | acl-name } [ rule rule ] }*

View

System view

Parameter

user-group { acl-number | acl-name }: activate the user-defined ACL. acl-number: Specifies the ACL number, ranging from 5000 to 5999. acl-name: Specifies the ACL name with a character string started with English letters (that is [a to z, A to Z]), excluding space and quotation marks.

ip-group { acl-number | acl-name }: activate the IP ACLs. IP ACLs include basic, advanced ACLs. acl-number: Specifies the ACL number, ranging from 2000 to 3999. acl-name: Specifies the ACL name with a character string started with English letters (that is [a to z, A to Z]), excluding space and quotation marks.

link-group { acl-number | acl-name }: activate the L2 ACL. acl-number: Specifies the ACL number, ranging from 4000 to 4999. acl-name: Specifies the ACL name with a character string started with English letters (that is [a to z, A to Z]), excluding space and quotation marks.

rule rule: Specifies the rule in the ACL to be activated, ranging from 0 to 127. If it is not specified, all the rules in the ACL will be activated.

Description

Using packet-filter command, you can activate the ACL. Using undo packet-filter command, you can disable the ACL.

This command supports activating the Layer-2 and Layer-3 ACLs at the same time. However, the actions of the ACLs should be consistent. If the actions conflict (one is permit and the other is deny), they cannot be activated.

Example

# Activate ACL 2000.
[Quidway] packet-filter ip-group 2000

1.1.6 reset acl counter

Syntax

reset acl counter { all | acl-number | acl-name }

View

User view
Parameter

`all`: All the access lists (including numbered and named access lists).

`acl-number`: Specifies an access list with a number in the range of 2000 and 3999.

`acl-name`: Specifies an access list with a character string, beginning with English letters [a-z, A-Z] only, excluding space and quotation marks, and not case sensitive. The `all` and `any` keywords are not allowed.

Description

Using the `reset acl counter` command, you can reset the statistics information of the ACL which is used to filter or classify the data treated by the software of switch. You can clear the matched counters to zero using this command.

**Table 1-5 The comparison between reset commands of statistics information**

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>reset acl counter</code></td>
<td>Reset the statistics information of the ACL which is used in the case of filtering or classifying the data treated by the software of switch. The case includes: ACL cited by route policy function, ACL used for control logon user, etc. The ACL number ranges from 2000 to 3999.</td>
</tr>
<tr>
<td><code>reset traffic-statistic</code></td>
<td>Reset statistic information of traffic. This command is used in the case of filtering or classifying the data transmitted by the hardware of switch. Commonly, this command is used to reset the statistics information of the <code>traffic-statistic</code> command.</td>
</tr>
</tbody>
</table>

Example

```bash
# Clear the statistics information of ACL 2000.
<Quidway> reset acl counter 2000
```

1.1.7 rule

Syntax

1. define/delete a rule for basic acl

```
rule [ rule-id ] { permit | deny } [ source { source-addr wildcard | any } | fragment | time-range name ]
undo rule rule-id [ source | fragment | time-range ]
```

Huawei Technologies Proprietary
II. define/delete a rule for advanced acl

```
rule [ rule-id ] { permit | deny } protocol [ source { source-addr wildcard | any } ]
[ destination { dest-addr dest-mask | any } ] [ source-port operator port1 [ port2 ] ]
[ destination-port operator port1 [ port2 ] ] [ icmp-type type code ] [ established ]
[ [ precedence precedence | tos tos ] | dscp dscp ] [ fragment ] [ time-range name ]
undo rule rule-id [ destination | destination-port | dscp | fragment | icmp-type |
precedence | source | source-port | time-range | tos ]*
```

III. define/delete a rule for link acl

```
rule [ rule-id ] { permit | deny } [ protocol ] [ cos vlan-pri ] [ ingress { { source-vlan-id |
source-mac-addr source-mac-wildcard } | interface { interface-name | interface-type |
interface-num } }* | any } ] [ egress { { dest-mac-addr dest-mac-wildcard | interface |
interface-name | interface-type interface-num } }* | any } ] [ time-range name ]
undo rule rule-id
```

IV. define/delete a rule for user-defined acl

```
rule [ rule-id ] { permit | deny } [ rule-string rule-mask offset ] &<1-8> [ time-range |
name ]
undo rule rule-id
```

View

ACL view

Parameter

- `rule-id`: Specifies a rule of an ACL with a number in the range of 0 to 127.
- `permit`: Indicates to let the matched packets through.
- `deny`: Indicates to reject the matched packets to pass through.
- `time-range name`: Name of a time range, during which a rule takes effect.

---

**Note:**
The following parameters are attributes carried by the data packets. The ACL rules are defined according to the values of these parameters.

- The parameter for define a basic ACL

  `source-addr wildcard | any`: `source-addr wildcard` is the source IP address and source address wildcard, expressed in dotted decimal notation. `any` represents any source address.
fragment: Indicates that the rule takes effect on fragmented packets only and will be ignored for other packets.

- The parameter of advanced ACL

protocol: This parameter is to define protocol type, which can be indicated by name, or digit. This parameter can be icmp, igmp, tcp, udp, ip, gre, ospf or ipinip. If this parameter takes ip, it means all the IP protocols. This parameter can be 1 ~ 255 if indicated by digit.

source-addr wildcard | any: source-addr wildcard is the source IP address and source address wildcard, expressed in dotted decimal notation. any represents any source address.

dest-addr wildcard | any: dest-addr wildcard is the destination IP address and destination address wildcard, expressed in dotted decimal notation. any represents any destination address.

source-port operator port1 [ port2 ]: This parameter is to define the source TCP or UDP port number. Here, operator represents port operation character, including eq (equal to), gt (greater than), lt (less than), neq (not equal to), and range (in certain range). Note: This parameter is available only when protocol parameter takes TCP or UDP. port1 [ port2 ]: TCP or UDP port number of packets, expressed with characters or numbers. The numbers are in the range of 0 to 65535 and refer to mnemonic symbol table for character values.

destination-port operator port1 [ port2 ]: This parameter is to define the destination TCP or UDP port number. The meaning of operator port1 [ port2 ] is same as upper parameter.

icmp-type type code: Used when protocol is specified as icmp. type code specifies an ICMP packet. type specifies the ICMP packet type with a number in the range of 0 to 255 or characters. code, ranging from 0 to 255, is used for icmp when ICMP packet type are not specified with characters.

established: Used when protocol is tcp to indicate that the rule takes effect on the first SYN packet to establish TCP connection.

precedence precedence: Specifies IP precedence with a number in the range of 0 to 7 or a name.

tos tos: Classifies the data packets with a number in the range of 0 to 15 or a name.

dscp dscp: Classifies the data packets with a number in the range of 0 to 63 or a name.

fragment: Indicates that the rule takes effect on fragmented packets only and will be ignored for other packets.

- The parameter of link ACL

protocol: Protocol carried by an Ethernet frame, which can be ip, arp, rarp, pppoe-control, or pppoe-data.
cos  

**cos**  

*vlan-pri*: 802.1p priority, ranging from 0 to 7.

**Ingress**  

{  
  {  
    {  
      source-vlan-id  |  source-mac-addr  source-mac-wildcard  
    }  
    interface  
    {  
      interface-name  |  interface-type  interface-num  
    }  
  }  
  |  any  

}: Source information of a data packet.  

- **source-vlan-id**: specifies the source VLAN of the packet, and  
- **source-mac-addr source-mac-wildcard**: specifies the source MAC address and MAC address wildcard of the data packets.  

These two parameters give the source MAC address range interested the users. For example, if **source-mac-wildcard** is specified as 0.0.ffff, it indicates that the user is interested in the first 32 bits (corresponding to the 0s in wildcard) of the source MAC address.  

**interface**  

{  
  interface-name  |  interface-type  interface-num  
}: represents the L2 port receiving the packets.  

**any** represents all the packets received from all the ports.

**Egress**  

{  
  {  
    dest-mac-addr  dest-mac-wildcard  
  }  
  |  interface  
  {  
    interface-name  |  interface-type  interface-num  
  }  
}: Specifies the destination information of data packets.  

- **dest-mac-addr dest-mac-wildcard**: specifies the destination MAC address and destination MAC address wildcard of the data packets. For example, if **dest-mac-wildcard** is specified as 0.0.ffff, it indicates that the user is interested in the first 32 bits (corresponding to the 0s in wildcard) of the destination MAC address.  

**interface**  

{  
  interface-name  |  interface-type  interface-num  
}: the L2 port forwarding the packets.  

**any** represents all the packets forwarded by all the ports.

- The parameter of user-defined ACL

{  
  rule-string  rule-mask  offset  
}:  

- **rule-string** is a character string of a rule defined by a user. It only consists of hexadecimal numbers of 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**

Using **rule** command, you can add a rule to an ACL. Using **undo rule** command, you can cancel a rule from an ACL.

You can add a lot of rules to an ACL. If you input the parameter when use the **undo rule** command, the system will delete the corresponding content of the rule according to the parameter input.

For related configurations, refer to command acl.

**Example**

# Add a rule to an advanced ACL.

[Quidway-acl-adv-3000]  
rule 1 permit tcp established source 1.1.1.1 0  
destination 2.2.2.2 0
# Add a rule to a basic ACL.
[Quidway-acl-basic-2000] rule 1 permit source 1.1.1.1 0 fragment

# Add a rule to an L2 ACL.
[Quidway-acl-link-4000] rule 1 permit ingress 1 egress any

# Add a rule to a user-defined ACL.
[Quidway-acl-user-5000] rule 1 permit 88 ff 18

### 1.1.8 time-range

**Syntax**

```
 time-range time-name { start-time to end-time days-of-the-week [ from start-time start-date ] [ to end-time end-date ] | from start-time start-date [ to end-time end-date ] }
```

**undo time-range time-name [ start-time to end-time days-of-the-week [ from start-time start-date ] [ to end-time end-date ] | from start-time start-date [ to end-time end-date ] ]**

**View**

System view

**Parameter**

- **time-name**: Name of a special time range to be referenced.
- **start-time**: Start time of the special time range, format as hh:mm.
- **end-time**: End time of the special time range, format as hh:mm.
- **days-of-the-week**: Determines in which day(s) of a week in the special time range a command takes effect. You can specify this parameter with any of the following values.
  - Numbers (ranging from 0 to 6);
  - Monday, Tuesday, Wednesday, Thursday, Friday, Saturday or Sunday;
  - working-day, representing 5 working days, from Monday to Friday;
  - off-day, representing Saturday and Sunday;
  - daily, representing everyday of the week.
- **from start-time start-date**: Start time and date of the special time range, determining effective days of the time range with the end-date, format as hh:mm MM-DD-YYYY.
- **to end-time end-date**: End time and date of the special time range, determining effective days of the time range with the start-date, format as hh:mm MM-DD-YYYY.
Description

Using **time-range** command, you can configure a time range. Using **undo time-range** command, you can delete a time range.

If you input the parameter when use the **undo time-range** command, the system will delete the corresponding content of the time range according to the parameter input.

Example

```
# Configure a time range being effective since zero hour on January 1, 2000 and forever.
[Quidway] time-range test from 0:0 1-1-2000
```
Chapter 2 QoS Commands

2.1 QoS Configuration Commands List

2.1.1 display qos cos-local-precedence-map

Syntax

display qos cos-local-precedence-map

View

Any view

Parameter

None

Description

Using **display qos cos-local-precedence-map** command, you can view “COS->Local-precedence” map.

Example

```
# Display "COS->Local -precedence" map.
<Quidway> display qos cos-local-precedence-map
cos-local-precedence-map:
    cos :  0 1 2 3 4 5 6 7
-----------------------------------------------
local-precedence :  2 0 1 3 4 5 6 7
```

2.1.2 display qos-global all

Syntax

**display qos-global all**

View

Any view

Parameter

None
Description

Using `display qos-global all` command, you can view the settings of all the QoS parameters.

This command is used for displaying the settings of all the QoS parameters, including priority tag, redirection, traffic statistics and traffic mirror.

Example

```bash
# Display the settings of all the QoS parameters.
[Quidway] display qos-global all

traffic-priority
  Matches: acl std1 rule 0 running
  Priority action: dscp ef
  Matches: acl std1 rule 1 running
  Priority action: dscp ef

traffic-redirect
  Matches: acl std1 rule 0 running
  Redirected to: interface Ethernet0/2
  Matches: acl std1 rule 1 running
  Redirected to: interface Ethernet0/2

traffic-statistic
  Matches: acl std1 rule 0 running
  0 byte
  0 packet
  Matches: acl std1 rule 1 running
  0 byte
  0 packet

mirrored-to
  Matches: acl std1 rule 0 running
  Mirrored to: Ethernet0/1
  Matches: acl std1 rule 1 running
  Mirrored to: Ethernet0/1
```
Table 2-1 the display Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>traffic-priority</td>
<td>Indicates the traffic-priority configuration of the switch.</td>
</tr>
<tr>
<td>Matches: acl std1 rule 0</td>
<td>“Matches: acl std1 rule 0 running” indicates the classification rule to the</td>
</tr>
<tr>
<td>Priority action: dscp ef</td>
<td>traffic.</td>
</tr>
<tr>
<td>Matches: acl std1 rule 1</td>
<td>“Priority action: dscp ef” indicates the action of resetting the priority of</td>
</tr>
<tr>
<td>Priority action: dscp ef</td>
<td>the packets matching the classification rule.</td>
</tr>
<tr>
<td>traffic-redirect</td>
<td>Indicates the traffic-redirect configuration of the switch.</td>
</tr>
<tr>
<td>Matches: acl std1 rule 0</td>
<td>“Matches: acl std1 rule 0 running” indicates the classification rule to the</td>
</tr>
<tr>
<td>Redirected to: interface</td>
<td>traffic.</td>
</tr>
<tr>
<td>Ethernet0/2</td>
<td>“Redirected to: interface Ethernet0/2” indicates the redirect port for the</td>
</tr>
<tr>
<td>Matches: acl std1 rule 1</td>
<td>packets matching the classification rule.</td>
</tr>
<tr>
<td>Redirected to: interface</td>
<td>Ethernet0/2</td>
</tr>
<tr>
<td>traffic-statistic</td>
<td>Indicates the traffic-statistic configuration of the switch.</td>
</tr>
<tr>
<td>Matches: acl std1 rule 0</td>
<td>“Matches: acl std1 rule 0 running” indicates the classification rule to the</td>
</tr>
<tr>
<td>0 byte</td>
<td>traffic.</td>
</tr>
<tr>
<td>0 packet</td>
<td>“0 byte 0 packet” indicates the statistic information for the packets</td>
</tr>
<tr>
<td>Matches: acl std1 rule 1</td>
<td>matching the classification rule.</td>
</tr>
<tr>
<td>0 byte</td>
<td></td>
</tr>
<tr>
<td>0 packet</td>
<td></td>
</tr>
<tr>
<td>mirrored-to</td>
<td>Indicates the mirroring configuration of the switch.</td>
</tr>
<tr>
<td>Matches: acl std1 rule 0</td>
<td>“Matches: acl std1 rule 0 running” indicates the classification rule to the</td>
</tr>
<tr>
<td>Mirrored to: Ethernet0/1</td>
<td>traffic.</td>
</tr>
<tr>
<td>Matches: acl std1 rule 1</td>
<td>“Mirrored to: Ethernet0/1” indicates the monitor port for the packets</td>
</tr>
<tr>
<td>Mirrored to: Ethernet0/1</td>
<td>matching the classification rule.</td>
</tr>
</tbody>
</table>

2.1.3 display qos-global mirrored-to

Syntax

```
display qos-global mirrored-to
```
View

Any view

Parameter

None

Description

Using **display qos-global mirrored-to** command, you can 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.

For the related command, see **mirrored-to**.

Example

# Display the settings of traffic mirror.
<Quidway> display qos-global mirrored-to
mirrored-to
   Matches: acl std1 rule 0 running
          Mirrored to: Ethernet0/1
   Matches: acl std1 rule 1 running
          Mirrored to: Ethernet0/1

Table 2-2 the display Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mirrored-to</td>
<td>Indicates the mirroring configuration of the switch.</td>
</tr>
<tr>
<td></td>
<td>&quot;Matches: acl std1 rule 0 running&quot; indicates the classification rule to the</td>
</tr>
<tr>
<td></td>
<td>traffic.</td>
</tr>
<tr>
<td>Mirrored to: Ethernet0/1</td>
<td>&quot;Mirrored to: Ethernet0/1&quot; indicates the monitor port for the packets</td>
</tr>
<tr>
<td></td>
<td>matching the classification rule.</td>
</tr>
</tbody>
</table>

2.1.4 **display qos-global traffic-priority**

Syntax

**display qos-global traffic-priority**

View

Any view
Parameter

None

Description

Using `display qos-global traffic-priority` command, you can view the settings of traffic priority.

This command is used for displaying the settings of traffic priority. The information displayed includes the ACL corresponding to the traffic tagged with priority, priority type and value.

For the related command, see `traffic-priority`.

Example

```bash
# Display the settings of traffic priority.
<Quidway> display qos-global traffic-priority
traffic-priority
  Matches: acl std1 rule 0 running
    Priority action: dscp ef
  Matches: acl std1 rule 1 running
    Priority action: dscp ef
```

Table 2-3 the display Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>traffic-priority</td>
<td>Indicates the traffic-priority configuration of the switch.</td>
</tr>
<tr>
<td>Matches: acl std1 rule 0 running</td>
<td>“Matches: acl std1 rule 0 running” indicates the classification rule to the traffic.</td>
</tr>
<tr>
<td>Priority action: dscp ef</td>
<td>“Priority action: dscp ef” indicates the action of resetting the priority of the packets matching the classification rule.</td>
</tr>
</tbody>
</table>

2.1.5 display qos-global traffic-redirect

Syntax

`display qos-global traffic-redirect`

View

Any view
Parameter

None

Description

Using **display qos-global traffic-redirect** command, you can view the settings of the redirection.

This command is used for displaying the settings of the redirection. The information displayed includes the ACL corresponding to the traffic to be redirected, the destination port of redirection.

For the related command, see **traffic-redirect**.

Example

```plaintext
# Display the settings of the redirection.
<Quidway> display qos-global traffic-redirect
traffic-redirect
| Matches: acl std1 rule 0 running |
| Redirected to: interface Ethernet0/2 |
| Matches: acl std1 rule 1 running |
| Redirected to: interface Ethernet0/2 |
```

Table 2-4 the display Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>traffic-redirect</td>
<td>Indicates the traffic-redirect configuration of the switch.</td>
</tr>
<tr>
<td>Matches: acl std1 rule 0 running</td>
<td>“Matches: acl 1 rule 0 running” indicates the classification rule to the traffic.</td>
</tr>
<tr>
<td>Redirected to: interface Ethernet0/2</td>
<td>“Redirected to: interface Ethernet0/2” indicates the redirect port for the packets matching the classification rule.</td>
</tr>
</tbody>
</table>

2.1.6 display qos-global traffic-statistic

Syntax

`display qos-global traffic-statistic`

View

Any view
Parameter

None

Description

Using `display qos-global traffic-statistic` command, you can view the traffic statistics information.

This command is used for displaying the traffic statistics information. The information displayed includes the ACL corresponding to the traffic to be counted and the number of packets counted.

The statistics information of `traffic-statistic` command includes the matched times of the transmitted data by switch. User can use `display qos-global traffic-statistic` command to display the statistics information.

For the related command, see `traffic-statistic`.

Example

# Display the traffic statistics information.
<Quidway> display qos-global traffic-statistic
traffic-statistic
Matches: acl std1 rule 0  running
  0 byte
  0 packet
Matches: acl std1 rule 1  running
  0 byte
  0 packets

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>traffic-statistic Matches: acl std1 rule 0 running</td>
<td>Indicates the traffic-statistic configuration of the switch.</td>
</tr>
<tr>
<td>0 byte</td>
<td>&quot;Matches: acl std1 rule 0 running&quot; indicates the classification rule to the traffic.</td>
</tr>
<tr>
<td>0 packet</td>
<td>&quot;0 byte 0 packet&quot; indicates the statistic information for the packets matching the classification rule.</td>
</tr>
</tbody>
</table>
2.1.7 display qos-interface all

Syntax

display qos-interface [ interface-name | interface-type interface-num ] all

View

Any view

Parameter

interface-name | interface-type interface-num: Specifies a port of the switch. For detailed information, refer to the port command manual.

Description

Using display qos-interface all command, you can view the QoS setting of all the ports.

If you do not input the port parameters, the command will display all the QoS settings on the switch, including traffic limit and line rate etc. If you set the port parameters, the configuration information about the specified port will be displayed.

Example

# Display the QoS settings of all the ports.
<Quidway> display qos-interface all
Ethernet0/2: traffic-limit
  Inbound:
    Matches: acl 2000 rule 0 running
    Target rate: 4 Mbps
    Exceed action: drop
Ethernet0/4: line-rate
  Line rate: 3 Mbps
Ethernet0/4: line-rate
  Line rate: 5 Mbps
Table 2-6 the display Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet0/2: traffic-limit Inbound:</td>
<td>Indicates the traffic-limit configuration of the port. “Inbound:&quot; indicates system only treats the traffic received by the port.</td>
</tr>
<tr>
<td>Matches: acl 2000 rule 0 running Target rate: 4 Mbps Exceed action: drop</td>
<td>“Matches: acl 2000 rule 0 running” indicates the classification rule to the traffic. “Target rate: 4 Mbps” indicates the normal rate for the packets matching the classification rule. “Exceed action: drop” indicates the action to the traffic which match the classification rule but exceed the normal rate. The action can be “drop” or “remark-dscp”.</td>
</tr>
<tr>
<td>Ethernet0/2: line-rate Line rate: 3 Mbps</td>
<td>Indicates the line-rate configuration of the port. “Line rate: 3 Mbps” indicates the general packet sending rate on a port.</td>
</tr>
</tbody>
</table>

2.1.8 display qos-interface line-rate

Syntax

```
display qos-interface [ interface-name | interface-type interface-num ] line-rate
```

View

Any view

Parameter

```
interface-name | interface-type interface-num: Specifies a port of the switch. For detailed information, refer to the port command manual.
```

Description

Using `display qos-interface line-rate` command, you can view the settings of outgoing line rate on the port.

If you do not input the port parameters, the command will display the outgoing line rate settings on the port. If you set the port parameters, the configuration information about the specified port will be displayed. The information displayed includes egress port and the line rate.

Example

```
# Display the line rate settings on the port.
[Quidway-Ethernet0/4] display qos-interface line-rate
Ethernet0/2: line-rate
```
Line rate: 3 Mbps
Ethernet0/4: line-rate
Line rate: 5 Mbps

**Table 2-7 the display Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet0/2: line-rate</td>
<td>Indicates the line-rate configuration of the port.</td>
</tr>
<tr>
<td>Line rate: 3 Mbps</td>
<td>“Line rate: 3 Mbps” indicates the general packet sending rate on a port.</td>
</tr>
</tbody>
</table>

2.1.9 **display qos-interface traffic-limit**

**Syntax**

```plaintext
display qos-interface [ interface-name | interface-type interface-num ] traffic-limit
```

**View**

Any view

**Parameter**

*interface-name | interface-type interface-num*: Specifies a port of the switch. For detailed information, refer to the port command manual.

**Description**

Using **display qos-interface traffic-limit** command, you can view the settings of traffic limit.

If you do not input the port parameters, the command will display the traffic limit settings on the switch. 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.

For the related command, see **traffic-limit**.

**Example**

# Display the settings of traffic limit.

```plaintext
<Quidway> display qos-interface traffic-limit
Ethernet0/1: traffic-limit
Inbound:
  Matches: acl 2000 rule 0 running
  Target rate: 10 Mbps
Ethernet0/2: traffic-limit
```
Inbound:
Matches: acl 2010 rule 0 running
Target rate: 100 Mbps
Exceed action: drop

Table 2-8 the display Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet0/2: traffic-limit</td>
<td>Indicates the traffic-limit configuration of the port.</td>
</tr>
<tr>
<td>Inbound:</td>
<td>“Inbound:” indicates system only treats the traffic received by the port.</td>
</tr>
<tr>
<td>Matches: acl 2000 rule 0 running</td>
<td>“Matches: acl 2000 rule 0 running” indicates the classification rule to the traffic.</td>
</tr>
<tr>
<td>Target rate: 4 Mbps</td>
<td>“Target rate: 4 Mbps” indicates the normal rate for the packets matching the classification rule.</td>
</tr>
<tr>
<td>Exceed action: drop</td>
<td>“Exceed action: drop” indicates the action to the traffic which match the classification rule but exceed the normal rate. The action can be “drop” or “remark-dscp”.</td>
</tr>
</tbody>
</table>

2.1.10 display queue-scheduler

Syntax

display queue-scheduler

View

Any view

Parameter

None

Description

Using **display queue-scheduler** command, you can view the queue scheduling mode and parameters.

For the related command, see **queue-scheduler**.

Example

```
# Display the queue scheduling mode and parameters.
<Quidway> display queue-scheduler
Queue scheduling mode: strict-priority

The display information shows the queue scheduling mode of the switch is Strict-Priority.
```
2.1.11 line-rate

Syntax

line-rate target-rate
undo line-rate

View

Ethernet port view

Parameter

target-rate: Specifies the general packet sending rate on a port, ranging from 1 to 100 measured in Mbps.

Description

Using line-rate command, you can configure the limitation of the rate to restrict the general speed of sending packets through the port. Using undo line-rate command, you can cancel the limitation of the rate.

This command is used for configuring the general limitation of rate on the port for sending packets.

Example

# Limit the rate on port e0/1 to 10Mbps.
[Quidway-Ethernet0/1] line-rate 10

2.1.12 mirrored-to

Syntax

mirrored-to { user-group acl-number | acl-name [ rule rule ] } | { ip-group { acl-number | acl-name } [ rule rule ] | link-group { acl-number | acl-name } [ rule rule ] }* }  
undo mirrored-to { user-group acl-number | acl-name [ rule rule ] } | { ip-group { acl-number | acl-name } [ rule rule ] | link-group { acl-number | acl-name } [ rule rule ] }* }

View

System view

Parameter

user-group { acl-number | acl-name } [ rule rule ]: Specifies a user-defined ACL.  
acl-number: Specifies the ACL sequence number, ranging from 5000 to 5999.  
accl-name: Specifies the ACL name with a character string starting with English letters
(a-z, A-Z) and excluding space and quotation mark. **rule rule**: Specifies a rule of an ACL, ranging from 0 to 127. If you do not set this parameter, all the rules will be considered.

**ip-group { acl-number | acl-name } [ rule rule ]**: Specifies a basic or advanced ACL. **acl-number**: Specifies the ACL sequence number, ranging from 2000 to 3999. **acl-name**: Specifies the ACL name with a character string starting with English letters ([a-z, A-Z]) and excluding space and quotation mark. **rule rule**: Specifies a rule of an ACL, ranging from 0 to 127. If you do not set this parameter, all the rules will be considered.

**link-group { acl-number | acl-name } [ rule rule ]**: Specifies a Layer-2 ACL. **acl-number**: Specifies the ACL sequence number, ranging from 4000 to 4999. **acl-name**: Specifies the ACL name with a character string starting with English letters ([a-z, A-Z]) and excluding space and quotation mark. **rule rule**: Specifies a rule of an ACL, ranging from 0 to 127. If you do not set this parameter, all the rules will be considered.

**interface { interface-name | interface-type interface-num }**: Specifies the destination port where the traffic will be mirror. **interface-num** specifies the port number. **interface-num** and **interface-type** specify a complete port name together. **interface-name** is **interface-type** added with **interface-num**.

**Description**

Using **mirrored-to** command, you can enable ACL traffic identification and perform traffic mirror. Using **undo mirrored-to** command, you can cancel traffic mirror.

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.

For the related command, see **display qos-global mirrored-to**.

**Example**

```
# Mirrors the packets matching the ACL 2000 rules, whose action is permit, to the port Ethernet0/1.
[Quidway] mirrored-to ip-group 2000 interface e0/1
```

**2.1.13 priority**

**Syntax**

```
priority priority-level
undo priority
```
Parameter

(priority-level): Specifies the priority level of the port, ranging from 0 to 7.

Description

Using **priority** command, you can configure the priority of Ethernet port. Using **undo priority** command, you can restore the default port priority.

By default, the priority level of the port is 0 and switch replaces the 802.1p priority carried by a packet with the port priority.

Every port of Ethernet switch supports four packet egress queues. The switch puts the packets into different egress queues according to their priorities.

You can set a priority for a port and replace the 802.1p priority carried in the packet with it. After transmitting a packet, the switch will replace the packet 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 Ethernet0/1 port to 7.
[Quidway-Ethernet0/1] priority 7
```

2.1.14 priority trust

Syntax

```
priority trust
undo priority
```

Description

Using **priority trust** command, you can configure system trusting the packet 802.1p priority and not replacing the 802.1p priorities carried by the packets with the port priority. Using **undo priority** command, you can configure the system not trust 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 system trusting the packet 802.1p priority and not replacing the 802.1p priorities carried by the packets with the port priority.
[Quidway-Ethernet0/1] priority trust
```

## 2.1.15 `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`: Specifies the mapping value of “COS 0->local-prec”, which ranges from 0 to 7.
- `cos1-map-local-prec`: Specifies the mapping value of “COS 1->local-prec”, which ranges from 0 to 7.
- `cos2-map-local-prec`: Specifies the mapping value of “COS 2->local-prec”, which ranges from 0 to 7.
- `cos3-map-local-prec`: Specifies the mapping value of “COS 3->local-prec”, which ranges from 0 to 7.
- `cos4-map-local-prec`: Specifies the mapping value of “COS 4->local-prec”, which ranges from 0 to 7.
- `cos5-map-local-prec`: Specifies the mapping value of “COS 5->local-prec”, which ranges from 0 to 7.
- `cos6-map-local-prec`: Specifies the mapping value of “COS 6->local-prec”, which ranges from 0 to 7.
- `cos7-map-local-prec`: Specifies the mapping value of “COS 7->local-prec”, which ranges from 0 to 7.
Description

Using `qos cos-local-precedence-map` command, you can configure “COS -> Local-precedence” map. Using `undo qos cos-local-precedence-map` command, you can restore its default value.

By default, the system provides the default “COS -> Local-precedence” mapping relationship.

Table 2-9 The default “COS -> Local-precedence” map

<table>
<thead>
<tr>
<th>COS Value</th>
<th>Local Precedence</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
</tr>
</tbody>
</table>

If needed, you can change “COS -> Local-precedence” map using the command.

Example

# Configure “COS -> Local-precedence” map.

```
[Quidway] qos cos-local-precedence-map 0 1 2 3 4 5 6 7
```

After the configuration, the “COS -> Local-precedence” map is shown in Table 2-10.

Table 2-10 “COS -> Local-precedence” map

<table>
<thead>
<tr>
<th>COS Value</th>
<th>Local Precedence</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
</tr>
</tbody>
</table>
2.1.16 queue-scheduler

Syntax

```
queue-scheduler { strict-priority | wrr queue1-weight queue2-weight queue3-weight queue4-weight | wrr-max-delay queue1-weight queue2-weight queue3-weight queue4-weight maxdelay }
undo queue-scheduler
```

View

System view

Parameter

- **strict-priority**: Configures to perform strict priority scheduling.
- **wrr** `queue1-weight queue2-weight queue3-weight queue4-weight`: Configures to perform WRR scheduler. `queue1-weight`: Specifies the weight (percent of bandwidth assigned) 1. `queue2-weight`: Specifies the weight of the queue 2. `queue3-weight`: Specifies the weight of the queue 3. `queue4-weight`: Specifies the weight of the queue 4.
- **wrr-max-delay** `queue1-weight queue2-weight queue3-weight queue4-weight maxdelay`: Configures to perform Delay bounded WRR scheduler. `queue1-weight`: Specifies the weight (percent of bandwidth assigned) 1. `queue2-weight`: Specifies the weight of the queue 2. `queue3-weight`: Specifies the weight of the queue 3. `queue4-weight`: Specifies the weight of the queue 4. `maxdelay`: Specifies the maximum delay, ranging from 1 to 255, unit is 16ms. The packets in the highest-priority queue will be transmitted directly when the maximum delay expires.

Description

Using **queue-scheduler** command, you can configure the queue scheduler and the related parameters. Using **undo queue-scheduler** command, you can restore the default queue scheduler.

By default, the value is **strict-priority**.

For WRR and Delay bounded WRR, the sum of all the weights should equal 100.

For the related command, see **display queue-scheduler**.

Example

```
# Configure to perform WRR with the weights of the four queues as 20, 20, 30 and 30 respectively.
[Quidway] queue-scheduler wrr 20 20 30 30
```
2.1.17  reset traffic-statistic

Syntax

```
reset traffic-statistic { all | user-group { acl-number | acl-name } [ rule rule ] | { ip-group { acl-number | acl-name } [ rule rule ] | link-group { acl-number | acl-name } [ rule rule ] )* }
```

View

User view

Parameter

- **all**: Indicates to clear all the traffic statistics information of the ACLs configured with this function (including the combination items).

- **user-group { acl-number | acl-name } [ rule rule ]**: Specifies a user-defined ACL.
  - **acl-number**: Specifies the ACL sequence number, ranging from 5000 to 5999.
  - **acl-name**: Specifies the ACL name with a character string starting with English letters ([a-z, A-Z]) and excluding space and quotation mark. **rule rule**: Specifies a rule of an ACL, ranging from 0 to 127. If you do not set this parameter, all the rules will be considered.

- **ip-group { acl-number | acl-name } [ rule rule ]**: Specifies a basic or advanced ACL.
  - **acl-number**: Specifies the ACL sequence number, ranging from 2000 to 3999.
  - **acl-name**: Specifies the ACL name with a character string starting with English letters ([a-z, A-Z]) and excluding space and quotation mark. **rule rule**: Specifies a rule of an ACL, ranging from 0 to 127. If you do not set this parameter, all the rules will be considered.

- **link-group { acl-number | acl-name } [ rule rule ]**: Specifies a Layer-2 ACL.
  - **acl-number**: Specifies the ACL sequence number, ranging from 4000 to 4999,
  - **acl-name**: Specifies the ACL name with a character string starting with English letters ([a-z, A-Z]) and excluding space and quotation mark. **rule rule**: Specifies a rule of an ACL, ranging from 0 to 127. If you do not set this parameter, all the rules will be considered.

Description

Using **reset traffic-statistic** command, you can reset the traffic statistics information.
This command is used for clearing the statistics information about all the traffic or a specified one.
Table 2-11 The comparison between reset commands of statistics information

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>reset acl counter</td>
<td>Reset the statistics information of the ACL which is used in the case of filtering or classifying the data treated by the software of switch. The case includes: ACL cited by route policy function, ACL used for control logon user, etc. The ACL number ranges from 2000 to 3999.</td>
</tr>
<tr>
<td>reset traffic-statistic</td>
<td>Reset statistic information of traffic. This command is used in the case of filtering or classifying the data transmitted by the hardware of switch. Commonly, this command is used to reset the statistics information of the traffic-statistic command.</td>
</tr>
</tbody>
</table>

Example

```bash
# Clear the statistics information about ACL 2000.
<Quidway> reset traffic-statistic ip-group 2000
```

2.1.18 traffic-limit

Syntax

```bash
traffic-limit inbound { user-group { acl-number | acl-name } [ rule rule ] [ ip-group { acl-number | acl-name } [ rule rule ] [ link-group { acl-number | acl-name } [ rule rule ] [ link-group { acl-number | acl-name } [ rule rule ] ] ] ] | [ target-rate [ exceed action ] ] }* 
undo traffic-limit inbound { user-group { acl-number | acl-name } [ rule rule ] [ ip-group { acl-number | acl-name } [ rule rule ] [ link-group { acl-number | acl-name } [ rule rule ] ] ] | [ target-rate [ exceed action ] ] }*
```

View

Ethernet port view

Parameter

**inbound**: Configures to limit the rate of traffic received via the interface.

**user-group { acl-number | acl-name } [ rule rule ]**: Specifies a user-defined ACL.

**acl-number**: Specifies the ACL sequence number, ranging from 5000 to 5999.

**acl-name**: Specifies the ACL name with a character string starting with English letters ([a-z, A-Z]) and excluding space and quotation mark.

**rule rule**: Specifies a rule of an ACL, ranging from 0 to 127. If you do not set this parameter, all the rules will be considered.

**ip-group { acl-number | acl-name } [ rule rule ]**: Specifies a basic or advanced ACL.

**acl-number**: Specifies the ACL sequence number, ranging from 2000 to 3999.

**acl-name**: Specifies the ACL name with a character string starting with English letters
(a-z, A-Z) and excluding space and quotation mark. **rule rule**: Specifies a rule of an ACL, ranging from 0 to 127. If you do not set this parameter, all the rules will be considered.

**link-group** { acl-number | acl-name } [ rule rule ]: Specifies a Layer-2 ACL. **acl-number**: Specifies the ACL sequence number, ranging from 4000 to 4999, **acl-name**: Specifies the ACL name with a character string starting with English letters (a-z, A-Z) and excluding space and quotation mark. **rule rule**: Specifies a rule of an ACL, ranging from 0 to 127. If you do not set this parameter, all the rules will be considered.

**target-rate**: Specifies the normal rate, measured in mbps, ranging from 1 to 100.

**exceed action**: Specifies the action executed when the traffic exceeds the set rate, which include:
- **drop**: Drop the packet;
- **remark-dscp value**: Set a new DSCP value.

### Description

Using **traffic-limit** command, you can enable ACL traffic identification and perform limiting the rate of the traffic matching the specified ACL (whose action is permit). Using **undo traffic-limit** command, you can cancel the traffic limit.

### Example

# Limit rate of the traffic matching the ACL 2000 rules on Ethernet0/1, whose action is permit. The normal traffic rate is set to 50Mbps. Drop the packets exceeding the traffic. The local preference of the packets within the traffic range is set to 0.

[Quidway-Ethernet0/1] traffic-limit inbound ip-group 2000 50 exceed drop

### 2.1.19 traffic-priority

#### Syntax

```
traffic-priority { user-group { acl-number | acl-name } [ rule rule ] | { ip-group { acl-number | acl-name } [ rule rule ] | link-group { acl-number | acl-name } [ rule rule ] }* | { dscp dscp-value | ip-precedence { pre-value | from-cos } } | cos { pre-value | from-ipprec } | local-precedence pre-value }*
```

```
undo traffic-priority { user-group { acl-number | acl-name } [ rule rule ] | { ip-group { acl-number | acl-name } [ rule rule ] | link-group { acl-number | acl-name } [ rule rule ] }* }
```

#### View

System view
Parameter

user-group { acl-number | acl-name } [ rule rule ]: Specifies a user-defined ACL.
  acl-number: Specifies the ACL sequence number, ranging from 5000 to 5999.
  acl-name: Specifies the ACL name with a character string starting with English letters
  ([a-z, A-Z]) and excluding space and quotation mark. rule rule: Specifies a rule of an
  ACL, ranging from 0 to 127. If you do not set this parameter, all the rules will be
  considered.

ip-group { acl-number | acl-name } [ rule rule ]: Specifies a basic or advanced ACL.
  acl-number: Specifies the ACL sequence number, ranging from 2000 to 3999.
  acl-name: Specifies the ACL name with a character string starting with English letters
  ([a-z, A-Z]) and excluding space and quotation mark. rule rule: Specifies a rule of an
  ACL, ranging from 0 to 127. If you do not set this parameter, all the rules will be
  considered.

link-group { acl-number | acl-name } [ rule rule ]: Specifies a Layer-2 ACL. acl-number:
  Specifies the ACL sequence number, ranging from 4000 to 4999, acl-name: Specifies
  the ACL name with a character string starting with English letters ([a-z, A-Z]) and
  excluding space and quotation mark. rule rule: Specifies a rule of an ACL, ranging
  from 0 to 127. If you do not set this parameter, all the rules will be considered.

dscp dscp-value: Specifies DSCP preference, ranging from 0 to 63.

ip-precedence { pre-value | from-cos } : Specifies IP preference. pre-value specifies
  the IP preference, ranging from 0 to 7. from-cos indicates to set the IP preference to
  the same as that of 802.1p of the packet.

cos { pre-value | from-ipprec } : Specifies 802.1p preference. pre-value specifies the
  802.1p preference, ranging from 0 to 7. from-ipprec indicates to set the 802.1p
  preference to the same as IP preference.

local-precedence pre-value: Specifies the local preference, ranging from 0 to 7.

Description

Using traffic-priority command, you can activate ACL and tag the traffic priority
(whose action is permit). Using undo traffic-priority command, you can cancel the
  traffic priority settings.

It can mark three priorities (dscp/IP preference, and cos) for the packets. The switch
  can put the packets into egress queue according to the cos value (namely the 802.1p
  preference) or local preference. If both 802.1p preference and local preference are set,
  the switch will use the 802.1p preference first.

For the related command, see display qos-global traffic-priority.

Example

# Marks the priority for the packets matching the permit rules of ACL 2000. It sets the
  local preference to 0:
2.1.20 traffic-redirect

Syntax

```
traffic-redirect { user-group { acl-number | acl-name } [ rule rule ] | { ip-group { acl-number | acl-name } [ rule rule ] | link-group { acl-number | acl-name } [ rule rule ]}* } { cpu | interface { interface-name | interface-type interface-num } } 
undo traffic-redirect { user-group { acl-number | acl-name } [ rule rule ] | { ip-group { acl-number | acl-name } [ rule rule ] | link-group { acl-number | acl-name } [ rule rule ]}* }
```

View

System view

Parameter

```
user-group { acl-number | acl-name } [ rule rule ]: Specifies a user-defined ACL. 
acl-number: Specifies the ACL sequence number, ranging from 5000 to 5999. 
acl-name: Specifies the ACL name with a character string starting with English letters (\[a-z, A-Z\]) and excluding space and quotation mark. rule rule: Specifies a rule of an ACL, ranging from 0 to 127. If you do not set this parameter, all the rules will be considered.

ip-group { acl-number | acl-name } [ rule rule ]: Specifies a basic or advanced ACL. 
acl-number: Specifies the ACL sequence number, ranging from 2000 to 3999. 
acl-name: Specifies the ACL name with a character string starting with English letters (\[a-z, A-Z\]) and excluding space and quotation mark. rule rule: Specifies a rule of an ACL, ranging from 0 to 127. If you do not set this parameter, all the rules will be considered.

link-group { acl-number | acl-name } [ rule rule ]: Specifies a Layer-2 ACL. acl-number: Specifies the ACL sequence number, ranging from 4000 to 4999, acl-name: Specifies the ACL name with a character string starting with English letters (\[a-z, A-Z\]) and excluding space and quotation mark. rule rule: Specifies a rule of an ACL, ranging from 0 to 127. If you do not set this parameter, all the rules will be considered.

cpu: Configures to redirect the traffic to the CPU.

interface { interface-name | interface-type interface-num }: Specifies the Ethernet port to which the packets will be redirected. interface-type specifies the port type, which can be ethernet only. interface-num specifies the port number. interface-num and interface-type specify a complete port name together. interface-name is interface-type added with interface-num.
```
Description

Using `traffic-redirect` command, you can activate the ACL to recognize and redirect the traffic (whose action is `permit`). Using `undo traffic-redirect` command, you can cancel the redirection.

For the related command, see `display qos-global traffic-redirection`.

Example

```bash
# Redirects the packets matching the ACL 2000 rules with action permit to the port Ethernet0/1.
[Quidway] traffic-redirect ip-group 2000 interface e0/1
```

2.1.21 traffic-statistic

Syntax

```
traffic-statistic { user-group { acl-number | acl-name } [ rule rule ] | { ip-group { acl-number | acl-name } [ rule rule ] | link-group { acl-number | acl-name } [ rule rule ] }* }
```

```
undo traffic-statistic { user-group { acl-number | acl-name } [ rule rule ] | { ip-group { acl-number | acl-name } [ rule rule ] | link-group { acl-number | acl-name } [ rule rule ] }* }
```

View

System view

Parameter

```
user-group { acl-number | acl-name } [ rule rule ]: Specifies a user-defined ACL.
```

`acl-number`: Specifies the ACL sequence number, ranging from 5000 to 5999.

`acl-name`: Specifies the ACL name with a character string starting with English letters ([a-z, A-Z]) and excluding space and quotation mark. `rule rule`: Specifies a rule of an ACL, ranging from 0 to 127. If you do not set this parameter, all the rules will be considered.

```
ip-group { acl-number | acl-name } [ rule rule ]: Specifies a basic or advanced ACL.
```

`acl-number`: Specifies the ACL sequence number, ranging from 2000 to 3999.

`acl-name`: Specifies the ACL name with a character string starting with English letters ([a-z, A-Z]) and excluding space and quotation mark. `rule rule`: Specifies a rule of an ACL, ranging from 0 to 127. If you do not set this parameter, all the rules will be considered.

```
link-group { acl-number | acl-name } [ rule rule ]: Specifies a Layer-2 ACL.
```

`acl-number`: Specifies the ACL sequence number, ranging from 4000 to 4999. `acl-name`: Specifies the ACL name with a character string starting with English letters ([a-z, A-Z]) and excluding space and quotation mark. `rule rule`: Specifies a rule of a Layer-2 ACL, ranging from 0 to 127. If you do not set this parameter, all the rules will be considered.
excluding space and quotation mark. **rule rule**: Specifies a rule of an ACL, ranging from 0 to 127. If you do not set this parameter, all the rules will be considered.

**Description**

Using **traffic-statistic** command, you can activate the ACL to recognize and count the traffic (whose action is **permit**). Using **undo traffic-statistic** command, you can cancel the traffic statistics.

The statistics information of **traffic-statistic** command includes the matched times of the transmitted data by switch. User can use **display qos-global traffic-statistic** command to display the statistics information.

For the related command, see **display qos-global traffic-statistic**.

**Example**

# Count the packets matching the ACL 2000 rules with action permit.

[Quidway] traffic-statistic ip-group 2000
Chapter 3  Logon user’s ACL control command

3.1  Logon user’s ACL control command

3.1.1  acl

Syntax

\[ \text{acl acl-number} \{ \text{inbound} | \text{outbound} \} \]

View

User-interface view

Parameter

- **acl-number**: Specifies an ACL with a number in the range of 2000 to 3999.
- **inbound**: Perform ACL control over the users that telnet to the local switch.
- **outbound**: Perform ACL control over the users that telnet to other switches from the local switch.

Description

Using `acl` command, you can call an ACL and perform ACL control over the TELNET users.

This command calls numbered ACL only.

Example

\[
\# \text{Performs ACL control over the users that telnet to the local switch. (Suppose ACL 2020 has been defined.)} \\
[Quidway] \text{user-interface vty 0 4} \\
[Quidway-user-interface-vty0-4] \text{acl 2020 inbound}
\]

3.1.2  ip http acl

Syntax

\[ \text{ip http acl acl-number} \]

\[ \text{undo ip http acl} \]

View

System view
Parameter

\textit{acl-number}: Specifies a basic ACL with a number in the range of 2000 to 2999.

Description

Using \texttt{ip http acl} command, you can call an ACL and perform ACL control over the WEB network management users. Using \texttt{undo ip http acl} command, you can cancel the ACL control over the WEB network management users.

This command calls numbered basic ACL only.

Example

\begin{verbatim}
# Performs ACL control over the WEB network management users. (Suppose ACL 2020 has been defined.)
[Quidway] ip http acl 2020
\end{verbatim}

3.1.3 \texttt{snmp-agent community}

Syntax

\begin{verbatim}
snmp-agent community \{ read | write \} community-name \[ [ mib-view view-name ] \] \[ acl acl-number \] 
undo snmp-agent community community-name
\end{verbatim}

View

System view

Parameter

\texttt{read}: Indicate that MIB object can only be read.
\texttt{write}: Indicate that MIB object can be read and written.
\texttt{community-name}: Community name character string.
\texttt{mib-view view-name}: MIB view name.
\texttt{acl acl-number}: the number of basic ACL, ranging from 2000 to 2999.

Description

Using \texttt{snmp-agent community} command, you can configure the community name, and perform the ACL control over the network management user through the parameter \texttt{acl acl-number}. Using \texttt{undo snmp-agent community} command, you can cancel the configuration of community name.
Example

# Configures huawei as the community name, allows read-only access to the switch by the name, meanwhile, performs the ACL control to the network management user by ACL 2020. (Suppose ACL 2020 has been defined.)

[Quidway] snmp-agent community read huawei acl 2020

3.1.4 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: Configure to use V1 safe mode.

v2c: Configure to use V2c safe mode.

v3: Configure to use V3 safe mode.

groupname: Group name, ranging from 1 to 32 bytes.

read-view: Configures to allow read-only view settings.

readview: Read-only view name, ranging from 1 to 32 bytes.

write-view: Configure to allow read-write view settings.

writeview: Name of read-write view, ranging from 1 to 32 bytes.

notify-view: Configure to allow notify view settings.

notifyview: Specify the notify view name, ranging from 1 to 32 bytes.

acl acl-number: the number of basic ACL, ranging from 2000 to 2999

authentication: If this parameter is added to configuration command, the system will authenticate but not encrypt SNMP data packets.

privacy: Configure to authenticate and encrypt the packet.
Description

Using `snmp-agent group` command, you can configure a new SNMP group, and perform the ACL control to the group through the parameter `acl acl-number`. Using `undo snmp-agent group` command, you can cancel the SNMP group.

Example

```plaintext
# Creates a new SNMP group: huawei, and perform the ACL control to the group through ACL 2021. (Suppose ACL 2021 has been defined.)
[Quidway] snmp-agent group v1 huawei acl 2021
```

### 3.1.5 `snmp-agent usm-user`

**Syntax**

```plaintext
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 ] [ privacy-mode des56 priv-password ] [ acl acl-number ]
undo snmp-agent usm-user v3 user-name group-name { local | engineid engineid-string }
```

**View**

System view

**Parameter**

- **v1**: Configure to use V1 safe mode.
- **v2c**: Configure to use V2c safe mode.
- **v3**: Configure to use V3 safe mode.
- **username**: Specify the user name, ranging from 1 to 32 bytes.
- **groupname**: Specify the group name corresponding to that user, a character string at the length ranging from 1 to 32 bytes.
- **authentication-mode**: Specify the safety level as authentication required.
  - **md5**: Specify the authentication protocol as HMAC-MD5-96.
  - **sha**: Specify the authentication protocol as HMAC-SHA-96.
- **auth-password**: Specify the authentication password with a character string, ranging from 1 to 64 bytes.
- **privacy-mode**: Specify the safety level as encrypted.
- **des56**: Specify the authentication protocol as DES.
privpassword: Specify the encryption password with a character string, ranging from 1 to 64 bytes.

acl acl-number: the number of basic ACL, ranging from 2000 to 2999.

local: Local entity user.

engineid: Specify the related engine ID of the user.

Description

Using `snmp-agent usm-user` command, you can add a new user to a SNMP group, and perform the ACL control to the user through the parameter `acl acl-number`. Using `undo snmp-agent usm-user` command, you can cancel a user from corresponding SNMP group, meanwhile delete the configuration of ACL control.

Example

# Adds a user huawei for huaweigroup (an SNMP group), configures to authenticate with HMAC-MD5-96 and sets authentication password as hello, meanwhile perform the ACL control to the user through ACL 2020. (Suppose ACL 2020 has been defined.)
[Quidway] snmp-agent usm-user v3 huawei huaweigroup authentication-mode md5
[Quidway] snmp-agent usm-user v3 huawei huaweigroup privpassword hello
[Quidway] acl 2020
# Table of Contents

## Chapter 1 Stack Function Configuration Commands ................................................................. 1-1

1.1 Stack Function Configuration Commands ........................................................................... 1-1
   1.1.1 display stacking ........................................................................................................ 1-1
   1.1.2 stacking ................................................................................................................ 1-2
   1.1.3 stacking enable ....................................................................................................... 1-3
   1.1.4 stacking ip-pool ..................................................................................................... 1-3

## Chapter 2 HGMP V2 Configuration Commands .......................................................................... 2-1

2.1 NDP Configuration Commands ........................................................................................... 2-1
   2.1.1 display ndp ............................................................................................................ 2-1
   2.1.2 ndp enable ........................................................................................................... 2-4
   2.1.3 ndp timer hello ..................................................................................................... 2-5
   2.1.4 ndp timer aging .................................................................................................... 2-5
   2.1.5 reset ndp statistics ............................................................................................... 2-6

2.2 NTDP Configuration Commands ........................................................................................ 2-7
   2.2.1 display ntdp ......................................................................................................... 2-7
   2.2.2 display ntdp device-list ....................................................................................... 2-8
   2.2.3 ntdp enable .......................................................................................................... 2-10
   2.2.4 ntdp explore ........................................................................................................ 2-10
   2.2.5 ntdp hop .............................................................................................................. 2-11
   2.2.6 ntdp timer .......................................................................................................... 2-12
   2.2.7 ntdp timer hop-delay ......................................................................................... 2-12
   2.2.8 ntdp timer port-delay ......................................................................................... 2-13

2.3 Cluster Configuration Commands ....................................................................................... 2-14
   2.3.1 add-member ...................................................................................................... 2-14
   2.3.2 administrator-address ......................................................................................... 2-15
   2.3.3 auto-build ........................................................................................................... 2-15
   2.3.4 build ................................................................................................................... 2-16
   2.3.5 cluster ................................................................................................................ 2-17
   2.3.6 cluster enable .................................................................................................... 2-17
   2.3.7 cluster switch-to ................................................................................................. 2-18
   2.3.8 delete-member ................................................................................................. 2-19
   2.3.9 display cluster ................................................................................................... 2-20
   2.3.10 display cluster candidates ............................................................................... 2-22
   2.3.11 display cluster members ................................................................................. 2-23
   2.3.12 ftp-server ........................................................................................................ 2-25
   2.3.13 holdtime ........................................................................................................... 2-26
   2.3.14 ip-pool ............................................................................................................. 2-27
Chapter 2 Management Commands

2.3.15 logging-host ................................................................. 2-27
2.3.16 port-tagged ............................................................... 2-28
2.3.17 reboot member ........................................................... 2-29
2.3.18 snmp-host ................................................................. 2-29
2.3.19 tftp-server ................................................................. 2-30
2.3.20 timer ........................................................................ 2-31

Chapter 3 Multicast MAC Address for Cluster Management Commands .................. 3-1

3.1 Multicast MAC Address for Cluster Management Commands ............................. 3-1
3.1.1 cluster-mac ................................................................. 3-1
3.1.2 cluster-mac syn-interval ............................................... 3-1
Chapter 1 Stack Function Configuration Commands

1.1 Stack Function Configuration Commands

1.1.1 display stacking

Syntax

display stacking [ members ]

View

Any view

Parameter

members: Display stack member information. It is omitted for the slave switches.

Description

Using display stacking command, you can view the stack status information of the master switch or slave switches in a stack.

When using this command on the master switch without members, the displayed information will indicate that the local switch is the master switch and indicate the number of switches in the stack. Using the command with members, the member information of the stack will be displayed, including stack number of master/slave switches, stack name, stack device name, MAC address and status.

When using this command on a slave switch, the displayed information will indicate that the local switch is a slave switch of the stack, indicate the stack number of the switch and MAC address of the master switch in the stack.

Example

# Display the stack information on the master switch.
<stack_0.Quidway> display stacking
Main device for stack.
Total members: 2

# Display the stack member information on the master switch.
<stack_0.Quidway> display stacking members
Member number: 0
Name: stack_0.Quidway
Device: Quidway S3026c  
MAC Address: 00e0-fc07-0bc0  
Member status: Admin  
IP: 172.31.0.1/16

Member number: 1  
Name: stack_1.Quidway  
Device: Quidway S3026c  
MAC Address: 00e0-fc07-58a0  
Member status: Up  
IP: 172.31.0.2/16

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member number</td>
<td>The number of member switch, main device's number is 0</td>
</tr>
<tr>
<td>Name</td>
<td>Name of member switch</td>
</tr>
<tr>
<td>Device</td>
<td>Device type of member switch, such as S3526 etc.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Mac address of member switch.</td>
</tr>
<tr>
<td>Member status</td>
<td>Status of member switch, the member switch can be administrator or member.</td>
</tr>
<tr>
<td>IP: 172.31.0.1/16</td>
<td>IP address of member switch.</td>
</tr>
</tbody>
</table>

### 1.1.2 stacking

**Syntax**

`stacking num`

**View**

User view

**Parameter**

`num`: Number of the slave switch to be switched to.

**Description**

Using `stacking` command, you can switch from the master stack switch to a slave switch to perform the configuration.
This command can only be used to switch from the master switch to a slave switch and the user level remains the same while switching. To switch from a slave switch back to a master switch, input <quit>.

Example

# Switch from master switch Quidway to slave Switch1, perform the configuration on Switch1 and then switch back to the master switch.
<stack_0.Quidway> stacking 1
<stack_1.Quidway>
<stack_1.Quidway> quit
<stack_0.Quidway>

1.1.3 stacking enable

Syntax

stacking enable
undo stacking enable

View

System view

Parameter

None

Description

Using stacking enable command, you can establish a stack. Using undo stacking enable command, you can cancel the stack.

After entering this command, the system will automatically add the switches connected to the stack ports of the master switch to the stack. User can only operate on the master switch to delete a stack.

After a stack has been established, the slave switch will exit the stack automatically if the stack port is disconnected.

Example

# Establish a stack.
[Quidway] stacking enable

1.1.4 stacking ip-pool

Syntax

stacking ip-pool from-ip-address ip-address-number [ ip-mask ]
undo stacking ip-pool

View

System view

Parameter

from-ip-address: Starting address of the stack IP address pool.
ip-address-number: Number of IP address in the stack IP addresses pool.
ip-mask: Mask of the stack IP address.

Description

Using `stacking ip-pool` command, you can configure the optional IP address range in public network for a stack. Using `undo stacking ip-pool` command, you can restore to the default IP address configuration of the stack.

By default, no IP pool is configured.

Before establishing a stack, the user should firstly set the optional IP address range in the public network for a stack. Then the master switch will automatically distribute the applicable IP addresses for the slave switches to add to the stack.

This command can only be used on the non-stack switches. After a stack is established, the user will not be able to modify its IP address range.

`ip-address-number` must be larger than or equal to the maximum-number of stack switches. Otherwise, some switches cannot be added into the stack automatically.

Example

# Set the optional IP address range in public network for a stack.
[Quidway] stacking ip-pool 129.10.1.1 5
Chapter 2  HGMP V2 Configuration Commands

2.1  NDP Configuration Commands

2.1.1  display ndp

Syntax

display ndp [ interface port-list ]

View

Any view

Parameter

interface port-list: Specifies a list of ports isolated from the specified port. A list may contain consecutive or separated ports, or the combination of consecutive and separated ports. The parameter is expressed as { interface_type interface_num | interface_name } [ to { interface_type interface_num | interface_name } ] &<1-10>. interface_type specifies the port type. interface_num specifies the port number, expressed as slot number/port number. Key word to helps specify a port range.

Description

Using display ndp command, you can view global NDP configuration information, including NDP packet interval, NDP information hold time and neighbor information of all the ports.

Example

# Display global NDP configuration information.

[Quidway] display ndp

Neighbor Discovery Protocol is enabled.

Neighbor Discovery Protocol Ver: 1, Hello Timer: 60(s), Aging Timer: 180(s)

Interface: Ethernet0/1

Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: Ethernet0/2

Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: Ethernet0/3

Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0
Interface: Ethernet0/4
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: Ethernet0/5
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: Ethernet0/6
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: Ethernet0/7
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: Ethernet0/8
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: Ethernet0/9
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: Ethernet0/10
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: Ethernet0/11
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: Ethernet0/12
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: Ethernet0/13
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: Ethernet0/14
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: Ethernet0/15
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: Ethernet0/16
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: Ethernet0/17
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: Ethernet0/18
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0
Interface: Ethernet0/19
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: Ethernet0/20
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: Ethernet0/21
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: Ethernet0/22
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: Ethernet0/23
Status: Enabled, Pkts Snd: 11, Pkts Rvd: 12, Pkts Err: 0
Neighbor 1: Aging Time: 170(s)
MAC Address: 00e0-0003
Port Name: Ethernet0/23
Software Ver: VRP3.10
Device Name: Quidway S3526
Port Duplex: AUTO
Product Ver: 3526-0001C

Interface: Ethernet0/24
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet2/1
Status: Enabled, Pkts Snd: 4, Pkts Rvd: 5, Pkts Err: 0

Table 2-1 Information about NDP configuration the NDP neighbors discovered by a port

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor Discovery Protocol is enabled</td>
<td>The system NDP is enabled on the switch</td>
</tr>
<tr>
<td>Neighbor Discovery Protocol Ver: 1</td>
<td>The NDP version</td>
</tr>
<tr>
<td>Hello Timer: 60(s)</td>
<td>The current device transmits NDP packet every 60 seconds.</td>
</tr>
<tr>
<td>Aging Timer: 180(s)</td>
<td>A neighbor keeps the NDP information of the current device for 180 seconds.</td>
</tr>
<tr>
<td>Interface: Ethernet0/1</td>
<td>Port number, specify a port</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status: Enabled</td>
<td>NDP is enabled on the port</td>
</tr>
<tr>
<td>Pkts Snd: 89</td>
<td>Number of NDP packets transmitted from a port</td>
</tr>
<tr>
<td>Pkts Rvd: 262</td>
<td>Number of NDP packets received by a port</td>
</tr>
<tr>
<td>Pkts Err: 0</td>
<td>Number of error NDP packets received by a port</td>
</tr>
<tr>
<td>Neighbor 1: Aging Time: 170(s)</td>
<td>The neighbor NDP information aging time connected by the port</td>
</tr>
<tr>
<td>MAC Address</td>
<td>MAC address of a neighbor device</td>
</tr>
<tr>
<td>Port Name</td>
<td>Port name of a neighbor device</td>
</tr>
<tr>
<td>Software Ver</td>
<td>The software version of a neighbor device</td>
</tr>
<tr>
<td>Device Name</td>
<td>Device name of a neighbor device</td>
</tr>
<tr>
<td>Port Duplex</td>
<td>Port duplex mode of a neighbor device</td>
</tr>
<tr>
<td>Product Ver</td>
<td>The product version of a neighbor device</td>
</tr>
</tbody>
</table>

### 2.1.2 ndp enable

**Syntax**

```plaintext
ndp enable [ interface port-list ]
undo ndp enable [ interface port-list ]
```

**View**

System view or Ethernet port view

**Parameter**

`interface port-list`: Specifies a list of ports isolated from the specified port. A list may contain consecutive or separated ports, or the combination of consecutive and separated ports. The parameter is expressed as `{ interface_type interface_num | interface_name } [ to { interface_type interface_num | interface_name } ]` &<1-10>. `interface_type` specifies the port type. `interface_num` specifies the port number, expressed as slot number/port number. Key word to helps specify a port range.

**Description**

Using `ndp enable` command, you can enable NDP on a system in system view, or enable it on a port in Ethernet port view. Using `undo ndp enable` command, you can disable NDP on a system in system view, or disable it on a port in Ethernet port view.
Example

    # Enable system NDP.
    [Quidway] ndp enable

2.1.3 ndp timer hello

Syntax

    ndp timer hello seconds
    undo ndp timer hello

View

    System view

Parameter

    seconds: Specifies NDP packet interval and ranges from 5 to 254 in units of second. By default, NDP packets are transmitted every 60 seconds.

Description

    Using ndp timer hello command, you can configure how often to transmit the NDP packets. Using undo ndp timer hello command, you can restore the default NDP packet interval.

    A device shall refresh the NDP information of its adjacent nodes in time to maintain timely information as the adjacent nodes change. You can use configuration command to adjust the NDP refreshing frequency.

Example

    # Configure to transmit NDP packets every 80 seconds.
    [Quidway] ndp timer hello 80

2.1.4 ndp timer aging

Syntax

    ndp timer aging aging-in-secs
    undo ndp timer aging

View

    System view
**Parameter**

*aging-in-secs*: Specifies how often to refresh the neighbor node information on a port and ranges from 5 to 255 in units of second. By default, NDP is aged in 180 seconds.

**Description**

Using **ndp timer aging** command, you can configure how long a device will hold the NDP packets received from the local device. After the aging timer expires, the device will discard the received NDP neighbor node information. Using **undo timer aging** command, you can restore the default NDP information aging time.

A user can specify how long an adjacent device will hold the information of the local device. The adjacent device learns how long it will hold the NDP information from the aging time carried in NDP packets and discards the packets when the aging timer expires.

Normally NDP aging time is longer than NDP packet interface. Otherwise, the neighbor information table of an NDP port will become unstable.

**Example**

# Configure the aging time of NDP packet as 60, so that an adjacent device will discard the NDP packets from the local device 60 seconds after receiving them.  
[Quidway] ndp timer aging 60

2.1.5 **reset ndp statistics**

**Syntax**

```
reset ndp statistics [ interface port-list ]
```

**View**

User view

**Parameter**

*interface port-list* Specifies a list of ports isolated from the specified port. A list may contain consecutive or separated ports, or the combination of consecutive and separated ports. The parameter is expressed as { *interface_type* interface_num | interface_name } [ to { *interface_type* interface_num | interface_name } ] &<1-10>.

*interface_type* specifies the port type. *interface_num* specifies the port number, expressed as slot number/port number. Key word **to** helps specify a port range.

**Description**

Using **reset ndp statistics** command, you can reset the NDP counters to clear the NDP statistics information.
Example

# Clear NDP statistics information.
<Quidway> reset ndp statistics

2.2 NTDP Configuration Commands

2.2.1 display ntdp

Syntax

display ntdp

View

Any view

Parameter

None

Description

Using `display ntdp` command, you can view the global NTDP information. The displayed information includes collected hops, ntdp timer, hop-delay, port-delay and time taken for last collection.

This command is used for displaying the global NTDP information.

Example

# Display the global NTDP information.
[Quidway] display ntdp

NTDP is running.
Hops : 3
Timer : 0 min
Hop Delay : 200 ms
Port Delay: 20 ms
Last collection total time: 2216ms

Table 2-2 Description of global NTDP configuration information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTDP running</td>
<td>The global NTDP is enabled on the local device.</td>
</tr>
<tr>
<td>Hops</td>
<td>Hops for topology collection.</td>
</tr>
<tr>
<td>Timer</td>
<td>Interval of periodic topology collection.</td>
</tr>
<tr>
<td>Hop Delay</td>
<td>Delay that the device forwards topology collection request.</td>
</tr>
<tr>
<td>Port Delay</td>
<td>Delay that the port forwards topology collection request.</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>Last collection total time</td>
<td>Time taken by last collection.</td>
</tr>
</tbody>
</table>

### 2.2.2 display ntdp device-list

**Syntax**

```
display ntdp device-list [ verbose ]
```

**View**

All view

**Parameter**

*verbose*: Display the detailed information about the device.

**Description**

Using `display ntdp device-list` command, you can view the device information collected through NTDP.

**Example**

```
# Display the device list collected through NTDP.
<Quidway> display ntdp device-list

MAC          HOP   IP                        PLATFORM
00e0-fc10-0000 1    Quidway S3026c
00e0-fc07-3c00 3    Quidway S3026c
00e0-fc07-4de0 2 192.169.121.257/25 Quidway S3526
00e0-fc07-0bc0 0    Quidway S3526

# Display the detailed device information collected through NTDP.
<Quidway> display ntdp device-list verbose

Hostname : Quidway
MAC       : 00e0-fc10-0000
```

**Table 2-3** Description of device list information collected through NTDP

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC</td>
<td>MAC address of the device</td>
</tr>
<tr>
<td>HOP</td>
<td>Hops to the collecting device</td>
</tr>
<tr>
<td>PLATFORM</td>
<td>Platform information about device</td>
</tr>
<tr>
<td>IP</td>
<td>IP address and mask length of the VLAN1 on the device</td>
</tr>
</tbody>
</table>

Huawei Technologies Proprietary

2-8
Table 2-4 Description of detail information of devices collected through NTDP

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer MAC</td>
<td>MAC address of the peer device</td>
</tr>
<tr>
<td>Native Port ID</td>
<td>Name of local port connected to the peer device</td>
</tr>
<tr>
<td>Peer Port ID</td>
<td>Name of opposite port connected to the local device</td>
</tr>
<tr>
<td>Speed</td>
<td>Speed of the local port connected to the peer</td>
</tr>
<tr>
<td>Duplex</td>
<td>Duplex mode of the local port connected to the peer</td>
</tr>
</tbody>
</table>
2.2.3  ntdp enable

Syntax

ntdp enable
undo ntdp enable

View

System view/Ethernet port view

Parameter

None

Description

Using **ntdp enable** command, you can enable NTDP on switch or a port. Using **undo ntdp enable** command, you can disable NTDP on switch or a port.

By default, NTDP is enabled on switch and the ports supporting NDP. If NTDP is enabled on a port not supporting NDP, NTDP cannot run yet.

Before a device can process NTDP packet, the system NTDP must be enable first. After disabling system NTDP, all the NTDP information on the switch will be cleared and the switch will discard all the NTDP packets and stop transmitting NTDP request.

The user can use this command to enable/disable NTDP on a specified port to decide through which port to transmit/receive and forward NTDP packets. After the global NTDP and port NTDP have been enabled, the NTDP packets can be transmitted, received and forwarded via the port. After the NTDP is disabled on the port, the port will not process NTDP packets.

Sometimes it only needs collecting the topology connected to the downlink ports, not caring about that connected to the uplink. In this case, NTDP is supposed to be disabled on the uplink ports.

Example

```
# Enable NTDP on Ethernet0/1.
[Quidway-Ethernet0/1] ntdp enable
```

2.2.4  ntdp explore

Syntax

ntdp explore

View

User view
Parameter

None

Description

Using **ntdp explore** command, you can start topology information collection when you want to collect network topology information. NTDP will collect the NDP information of every device and all of their neighboring connections in the specified network scope. The administrator device or network management system will learn the network topology according to the information to manage and monitor the devices.

Example

```
# Start the topology collection.
<Quidway> ntdp explore
```

### 2.2.5 ntdp hop

**Syntax**

```
ntdp hop hop-value
undo ntdp hop
```

**View**

System view

**Parameter**

*hop-value*: Indicate the maximum hops that the device collected can be away from the topology collecting device, ranging from 1 to 16. By default, the value is 3.

**Description**

Using **ntdp hop** command, you can configure a limit to the hops for topology collection to collect the topology information of the devices among determined range, so that infinitive collection can be avoided. Using **undo ntdp hop** command, you can restore the default value. The limit is performed through controlling permitted hops from the originating of collection. For example, if you set a limit of 2 to the hop number, only the switches 2 hops away from the first switch transmitting the topology collection request will be collected.

This command is only effective on the topology-collecting device. The broader collection scope requires more memory of the topology-collecting device.

**Example**

```
# Set a limit of 5 hops for topology collection.
[Quidway] ntdp hop 5
```
2.2.6 ntdp timer

Syntax

```
ntdp timer interval-in-mins
undo ntdp timer
```

View

System view

Parameter

```
Interval-in-mins: The interval of collecting topology information periodically, ranging from 0 to 65535 in minutes. 0 indicates that no regular topology collection will be performed.
```

Description

Using `ntdp timer` command, you can configure the topology collection interval. Using `undo ntdp timer` command, you can restore the default topology collection interval.

By default, the interval of periodic topology collection is 0 minute, i.e. no regular topology collection will be performed.

In order to learn the topology changes in time, it is necessary to regularly collect the topology information throughout the whole scope specified. This can show any topological changes, some of which may be omitted by the partial collection.

Example

```
# Configure the periodic topology connection interval is 30 minutes.
[Quidway] ntdp timer 30
```

2.2.7 ntdp timer hop-delay

Syntax

```
ntdp timer hop-delay time
undo ntdp timer hop-delay
```

View

System view

Parameter

```
time: The time that the collected device wait before forwarding the topology-collection request, ranging from 1 to 1000 milliseconds. By default, the value is 200ms.
```
Description

Using `ntdp timer hop-delay` command, you can configure delay for collected device to forward topology collection request. Using `undo ntdp timer hop-delay` command, you can restore the default delay value.

To avoid network congestion resulted from collecting device’s receiving large amount of responses simultaneously, you can configure each collected device to delay response for a period of time after receiving the topology request. Then, the first port will start to forward the topology request packet.

This command is executed on the collecting device. The topology request contains the hop-delay time, according to which the collected device decides how long it shall wait before the first port forwards the request.

Example

```
# Configure that the collected device receives NTDP request and delays for 300ms before transmitting the NTDP packet to the first port.
[Quidway] ntdp timer hop-delay 300
```

2.2.8 ntdp timer port-delay

Syntax

```
ntdp timer port-delay time
undo ntdp timer port-delay
```

View

System view

Parameter

`time`: The delay before forwarding the topology request packet to the next port, ranging from 1 to 100 in milliseconds. By default, the value is 20ms.

Description

Using `ntdp timer port-delay` command, you can configure the delay before the next port’s forwarding packets on the collected device. Using `undo ntdp timer port-delay` command, you can restore the default port-delay.

To avoid network congestion resulted from collecting device’s receiving large amount of responses simultaneously, you can configure each collected device to delay response for a period of time after receiving the topology request. Then, the first port will start to forward the topology request packet.
This command is configured on the collecting device. The topology request contains the port-delay time, according to which the collected device decides how long it shall wait before the first port forwards the request.

Example

```
# Configure that the collected device shall delay for 40ms before the next port sends the request.
[Quidway] ntdp timer port-delay 40
```

### 2.3 Cluster Configuration Commands

#### 2.3.1 add-member

**Syntax**

```
add-member [member-num] mac-address H-H-H [ password password ]
```

**View**

Cluster view

**Parameter**

- `member-num`: Number of a member device, ranging from 1 to 256.
- `H-H-H`: The hexadecimal MAC address of a member device.
- `password`: The password of a candidate device. Before joining a cluster, the candidate device should be authenticated. A candidate without password need not input password. If password different from the password of the administrator device has been configured on the candidate device, a user has to input that password before adding the candidate device to the cluster.

**Description**

Using **add-member** command, you can add a candidate device to a cluster.

This command can be executed on the administrator device only. When adding a cluster member, you can use the `member-num` parameter to assign a member number to it at the same time. Remember to assign an unused number; otherwise, the system will prompt error. If you do not specify the member number, the administrator device will assign an unused one to the candidate.

A candidate with a password same as that of the administrator device or without password can join the cluster free from password authentication. Otherwise, the user has to input the password before adding the candidate.

Its device password will become the administrator device password if the candidate device is added to the cluster system.
Example

# Add the candidate device, with MAC address 00E0-fc00-35e7 and super-password huawei, to the cluster, and its member number is 6.

[Huawei_0.Quidway-cluster] add-member 6 mac-address 00E0-fc00-35e7 password huawei

2.3.2 administrator-address

Syntax

administrator-address mac-address name name
undo administrator-address

View

Cluster view

Parameter

mac-address: This parameter is to define MAC address of the administrator device.
name: Name of an existing cluster with no more than 8 characters, including only letters, digital, subtraction sign “-” and underline “_”.

Description

Using administrator-address command, you can store such information as administrator device address and cluster name related to a cluster on a member device and add a candidate to a cluster. Using undo administrator-address command, you can cancel a member from the cluster and make it a candidate again.

This command is used for saving configuration information. Generally a user does not need to use it. A member left the cluster through the undo administrator-address command will not notify the administrator device, and therefore you can still see such device on the administrator device yet it turns down. The right way to remove a cluster member is to execute the delete-member command.

Example

# Delete the current member device from the cluster.

[Quidway-cluster] undo administrator-address

2.3.3 auto-build

Syntax

auto-build [ recover ]
View

Cluster view

Parameter

recover: automatic get back the members of a cluster for the administrator device when it reboot.

Description

Using **auto-build** command, you can configure a cluster automatically.
This command can be used on a candidate device or an administrator device.
When you use this command on a candidate device, the system requires you to input a cluster name and creates a cluster. And then the cluster uses NTDP to collect candidates and adds them to the cluster upon your confirmation.
When you use this command on an administrator device, the system will collect the candidates directly.
The recover parameter is used for recover a cluster. Using the auto-build recover command, you can find the members left the member list and add them to the cluster again.
Note: Ensure that NTDP is enabled, because it is the basis of candidate and member collection. The collection range is also decided through NTDP. You can use **hop** command to decide the collection range in System view.
If a member has been configured with an enable-password different from the password of the administrator device, it cannot be added to a cluster automatically.

Example

```bash
# Set up a cluster automatically.
[Quidway-cluster] auto-build
```

2.3.4 **build**

Syntax

```bash
build name
undo build
```

View

Cluster view

Parameter

**name:** Cluster name with no more than 8 characters, including and only including letters, numerals, subtraction sign “-“ and underline “_“.
Description

Using **build** command, you can configure a cluster on a device. The *name* parameter specifies the name of the cluster. Using **undo build** command, you can cancel a cluster.

By default, all the devices supporting cluster are candidate devices.

After a cluster is created, the device on which the command is executed becomes the administrator device and will be assigned with a fixed member number of 0.

This command can be executed on an administrator device or a command-capable device. Using it on an administrator device, you can rename a cluster. Using it on a candidate device, you can create a cluster.

Example

```
# Configure the current switch as the administrator device and specifies HUAWEI as the cluster name.
[Quidway-cluster] build HUAWEI
```

2.3.5 cluster

Syntax

```
cluster
```

View

System view

Parameter

None

Description

Using **cluster** command, you can enter cluster view.

Example

```
# Enter cluster view.
[Quidway] cluster
[Quidway-cluster]
```

2.3.6 cluster enable

Syntax

```
cluster enable
undo cluster enable
```
View

System view

Parameter

None

Description

Using **cluster enable** command, you can enable the cluster function on a switch. Using **undo cluster enable** command, you can disable the cluster function of a switch.

By default, the cluster function is enabled on all the devices supporting cluster.

Above commands can be used on any device supporting the cluster function. When you use the **undo cluster enable** command on an administrator device, the system will delete the cluster and disable the cluster function on it. When you use it on a member device, the system will exit the cluster and disable the cluster function on it.

Note: If the cluster function is disabled, you cannot create a cluster on the device or add it to a cluster.

Example

```bash
# Enable the cluster function of a switch.
[Quidway] cluster enable
```

2.3.7 **cluster switch-to**

Syntax

```
cluster switch-to { member-num | mac-address H-H-H | administrator }
```

View

User view

Parameter

- **member-num**: Member number of member device, ranging from 1 to 256.
- **mac-address H-H-H**: MAC address of a member device.
- **administrator**: Redirect from a member device to the administrator device.

Description

Using **cluster switch-to** command, you can switch between administrator device and member devices for convenient management.

A member device in a cluster can be managed through the administrator device. The user can operate on an administrator device and switchover to a specified member

Huawei Technologies Proprietary

2-18
device for configuration management, or operate on a member device and switchover to an administrator device.

Authentication is required when the user switch from the administrator device to a member device. Upon passing the member device authentication, the switchover is allowed. If the password of the member device is different from the administrator device, the switchover will be rejected. The user level will be inherited from the administrator device when switching to the member device from administrator device. For example, the user view will remain as user view after switching from the administrator device to a member device.

Authentication is also required when you switch from a member device to the administrator device. After passing the authentication, the system will enter the user view automatically.

When executed on the administrator device, if the specified member number $n$ is omitted, the error message will be on display. Enter `quit` to stop the switchover operation.

**Example**

```plaintext
# Switch from the administrator device to member device 6 and then switches back to the administrator device.
<Huawei_0.Quidway> cluster switch-to 6
<Huawei_6.Quidway> quit
<Huawei_0.Quidway>
```

### 2.3.8 delete-member

**Syntax**

```
delete-member member-num
```

**View**

Cluster view

**Parameter**

`member-num`: Number of a member device, ranging from 1 to 255.

**Description**

Using `delete-member` command, you can cancel a member from the cluster. This command can be performed on administrator device. After performing this command, the administrator device will notify a member device to exit cluster and delete it from the member list. If the administrator device and the member device still cannot intercommunicate, the member will be deleted, however, the cluster information on the member device may not be deleted.
Example

# Delete the switch from cluster, its member number is 2.

[Huawei_0.Quidway-cluster] delete-member 2

2.3.9  display cluster

Syntax

display cluster

View

Any view

Parameter

None

Description

Using **display cluster** command, you can view the state and basic configuration information of the cluster.

This command can be performed on both administrator device and member device, but the displays are different. In the administrator device, there are cluster name, member number, handshake interval, holdtime, address pool, and the server of cluster. In the member device, there are member number, MAC address of administrator device, and the state of administrator device.

Example

# Display information about cluster on the administrator device.

<Quidway> display cluster
Cluster name:"sss"
Role:Administrator

Handshake timer:10 sec
Handshake hold-time:60 sec
IP-Pool:1.1.1.1/20
No logging host configured
No SNMP host configured
No FTP server configured
No TFTP server configured.
Table 2-5 Description of cluster status and statistics information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster name</td>
<td>Name of the cluster</td>
</tr>
<tr>
<td>Role</td>
<td>Role of the cluster member</td>
</tr>
<tr>
<td>Handshake timer</td>
<td>Value of handshake timer</td>
</tr>
<tr>
<td>Handshake hold-time</td>
<td>Value of handshake hold-time</td>
</tr>
<tr>
<td>IP-Pool</td>
<td>IP pool of the cluster</td>
</tr>
<tr>
<td>No logging host configured</td>
<td>The corresponding configuration of the cluster</td>
</tr>
<tr>
<td>No SNMP host configured</td>
<td></td>
</tr>
<tr>
<td>No FTP server configured</td>
<td></td>
</tr>
<tr>
<td>No TFTP server configured</td>
<td></td>
</tr>
</tbody>
</table>

# Display information about cluster on the member device.

```
<Quidway> display cluster
Cluster name:"sss"
Role:Member
Member number:1

Handshake timer:10 sec
Handshake hold-time:60 sec

Administrator device mac address:00e0-fc00-0003
Administrator status:Up
```

Table 2-6 Description of cluster status and statistics information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster name</td>
<td>Name of the cluster</td>
</tr>
<tr>
<td>Role</td>
<td>Role of the cluster member</td>
</tr>
<tr>
<td>Member state</td>
<td>Member status</td>
</tr>
<tr>
<td>Member number</td>
<td>Number of member device</td>
</tr>
<tr>
<td>Handshake timer</td>
<td>Value of handshake timer</td>
</tr>
<tr>
<td>Handshake hold-time</td>
<td>Value of handshake hold-time</td>
</tr>
<tr>
<td>Administrator device mac address</td>
<td>MAC address of administrator device</td>
</tr>
<tr>
<td>Administrator status</td>
<td>Status of administrator device</td>
</tr>
</tbody>
</table>
### 2.3.10 display cluster candidates

**Syntax**

```plaintext
display cluster candidates [ mac-address H-H-H | verbose ]
```

**View**

Any view

**Parameter**

- **mac-address H-H-H**: MAC address of candidate device.
- **verbose**: Display the detailed information about the candidate device.

**Description**

Using the `display cluster candidates` command, you can view candidate devices of the cluster.

This command can only be performed on the administrator device.

The candidate devices are collected by NTDP. Execute the `hop` command in System view to specify the collection range.

This command displays the candidate device collected by NTDP last time. In order to ensure the correctness of display, you can manually perform a collection first, or set the NTDP to run collection periodically.

**Example**

#### Display all the candidate devices lists.

```plaintext
<Quidway> display cluster candidates
```

<table>
<thead>
<tr>
<th>MAC</th>
<th>HOP</th>
<th>IP</th>
<th>PLATFORM</th>
</tr>
</thead>
<tbody>
<tr>
<td>00e0-fc10-0000</td>
<td>1</td>
<td></td>
<td>Quidway S3526</td>
</tr>
<tr>
<td>00e0-fc07-3c00</td>
<td>3</td>
<td></td>
<td>Quidway S3526</td>
</tr>
<tr>
<td>00e0-fc07-4de0</td>
<td>2</td>
<td>192.169.121.257/25</td>
<td>Quidway S3526</td>
</tr>
<tr>
<td>00e0-fc07-0bc0</td>
<td>0</td>
<td></td>
<td>Quidway S3526</td>
</tr>
</tbody>
</table>

#### Display the information about the specified candidate device.

```plaintext
<Quidway> display cluster candidates mac-address 00e0-fc61-c4c0
```

**Hostname**: LSW1

**MAC**: 00e0-fc61-c4c0

**Hop**: 1

**IP**: 1.5.6.9/16

**Platform**: Quidway S3526

#### Display the detailed information about all the candidate devices.

```plaintext
<Quidway> display cluster candidates verbose
```

**Hostname**: Quidway
MAC : 00e0-fc00-a01f
Hop : 2
IP:
Platform : Quidway S3026

Hostname : LSW1
MAC : 00e0-fc07-4de0
Hop : 1
IP: 1.5.6.7/16
Platform : Quidway S3526

Table 2-7 Description of candidate device list information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>Name of the candidate device</td>
</tr>
<tr>
<td>MAC</td>
<td>MAC address</td>
</tr>
<tr>
<td>Hop</td>
<td>Hops to the administrator device</td>
</tr>
<tr>
<td>IP</td>
<td>IP address</td>
</tr>
<tr>
<td>Platform</td>
<td>Platform of the candidate device</td>
</tr>
</tbody>
</table>

2.3.11 display cluster members

Syntax

display cluster members [member-num | verbose ]

View

Any view

Parameter

member-num: Cluster member number, ranging from 0 to 255.
verbose: Display the detailed information about all the member devices.

Description

Using display cluster command, you can view the information of cluster member. This command can only be performed on the administrator device. Using member-num or verbose parameter to display detail information of a certain member or all the members.

Example

# Display configuration information about the member devices.
<Quidway> display cluster members

<table>
<thead>
<tr>
<th>SN</th>
<th>Device</th>
<th>MAC Address</th>
<th>Status</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Quidway S3526</td>
<td>00e0-fc07-0bc0</td>
<td>Cmdr</td>
<td>Huawei_0.Quidway</td>
</tr>
<tr>
<td>1</td>
<td>Quidway S3026</td>
<td>00e0-fc00.a01f</td>
<td>Up</td>
<td>Huawei_1.Quidway</td>
</tr>
<tr>
<td>2</td>
<td>Quidway S3526</td>
<td>00e0-fc07-4de0</td>
<td>Up</td>
<td>Huawei_2.LSW1</td>
</tr>
</tbody>
</table>

Table 2-8 Description of detail information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SN</td>
<td>Device serial number</td>
</tr>
<tr>
<td>Device</td>
<td>Device type</td>
</tr>
<tr>
<td>MAC Address</td>
<td>MAC address of the device</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the device</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the device</td>
</tr>
</tbody>
</table>

# Display the detailed configuration information about the administrator device and all member devices.
<Quidway> display cluster members verbose

Member number: 0
Name: Huawei_0.Quidway
Device: Quidway S3526
MAC Address: 00e0-fc07-0bc0
Member status: Cmdr
Hops to administrator device: 0
IP: 1.1.200.210/16
Version:
Huawei Versatile Routing Platform Software
VRP (tm) Software, Version 3.10
Copyright (c) 2000-2002 By HUAWEI TECH CO., LTD.
Quidway S3526 3526-003

Member number: 1
Name: Huawei_1.Quidway
Device: Quidway S3026c
MAC Address: 00e0-fc00-a01f
Member status: Up
Hops to administrator device: 2
IP:
Version:
Huawei Versatile Routing Platform Software
VRP (tm) Software, Version 3.10
Table 2-9 Description of detail information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member number:</td>
<td>Device member number</td>
</tr>
<tr>
<td>Name:</td>
<td>Name of the device</td>
</tr>
<tr>
<td>Device:</td>
<td>Device type</td>
</tr>
<tr>
<td>MAC Address:</td>
<td>MAC address of the device</td>
</tr>
<tr>
<td>Member Status:</td>
<td>Status of the device</td>
</tr>
<tr>
<td>Hops to administrator device:</td>
<td>The hops from current member device to the administrator</td>
</tr>
<tr>
<td>IP:</td>
<td>IP address of current member device</td>
</tr>
<tr>
<td>Version:</td>
<td>Software Version of current device</td>
</tr>
</tbody>
</table>

2.3.12 ftp-server

Syntax

```plaintext
ftp-server ip-address
undo ftp-server
```

View

Cluster view

Parameter

`ip-address`: IP address of FTP server configured for the cluster.
Description

Using `ftp-server` command, you can configure the public FTP server for the cluster members on the administrator device. Using `undo ftp-server` command, you can configure administrator device as FTP server.

By default, the administrator device acts as FTP Server.

The member device within cluster will access FTP server via administrator device. Configure the IP address of FTP server for the cluster, then the member devices of the cluster can access the server via the administrator device.

Example

# Configure the IP address of FTP server for the cluster on the administrator device.

```
[Huawei_0.Quidway-cluster] ftp-server 1.0.0.9
```

2.3.13 holdtime

Syntax

```
holdtime seconds
undo holdtime
```

View

Cluster view

Parameter

`seconds`: Valid holdtime in seconds, ranging from 1 to 255. By default, the valid holdtime is 60 seconds.

Description

Using `holdtime` command, you can configure the valid holdtime of a switch. Using `undo holdtime` command, you can restore the default value of holdtime. After missing 3 times of handshake, if the switch still cannot receive any information of the peer device during holdtime, it will set the state of peer device to “down”. When the communication resumes, the relevant member device will be re-added to the cluster (automatically). If the downtime does not go beyond the valid holdtime specified by the user, the member device will stays in the normal state and need not be added again.

The commands can only be executed on the administrator device, which will advertise the cluster timer value to the member devices.

Example

# Set the cluster holdtime as 50 seconds.

```
[Huawei_0.Quidway-cluster] holdtime 50
```
2.3.14  ip-pool

Syntax

\[
\text{ip-pool administrator-ip-address \{} \ ip-mask | ip-mask-length \}\n\]

\[
\text{undo ip-pool}
\]

View

Cluster view

Parameter

- \text{administrator-ip-address}: IP address of the administrator device of the cluster.
- \text{ip-mask}: Mask of the cluster IP address pool.
- \text{ip-mask-length}: Mask length of the cluster IP address pool.

Description

Using \text{ip-pool} command, you can configure a private IP address range for a cluster on the command-switch-to-be. Using \text{undo ip-pool} command, you can restore the default IP address configuration of the cluster.

By default, no IP pool is configured.

Before setting up a cluster, the user should configure a private IP address pool for the member devices of the cluster. When a candidate device is added, the administrator device will dynamically assign a private IP address, which can be used for communication inside the cluster. In this way, the user can use the administrator device to manage and maintain the member devices.

The commands can only be executed on a switch of non-cluster member. The IP address pool of an existing cluster cannot be modified.

Example

\[
\# \text{Configure the IP address pool of a cluster.}
\]

\[
[\text{Quidway-cluster}] \text{ip-pool 10.200.0.1 20}
\]

2.3.15  logging-host

Syntax

\[
\text{logging-host ip-address}
\]

\[
\text{undo logging-host}
\]

View

Cluster view
Parameter

*ip-address*: IP address of logging host configured for the cluster.

Description

Using **logging-host** command, you can configure a public logging host for the member devices on the administrator device. Using **undo logging-host** command, you can cancel the logging host.

By default, there is no public logging host configured.

The commands are used to assign an IP address for the logging host of the cluster, thereby the members can send log information to logging host via the administrator device.

Example

```
# Configure the IP address of the logging host on the administrator device.
[Huawei_0.Quidway-cluster] logging-host 1.0.0.9
```

2.3.16 **port-tagged**

Syntax

```
port-tagged vlan vlanid
undo
undo port-tagged
```

View

Cluster view

Parameter

*vlanid*: ID of management VLAN, which can be configured as 1 only.

Description

Using **port-tagged** command, you can configure VLAN check for the communication inside a cluster on the administrator device. Using **undo port-tagged** command, you can cancel VLAN check for the communication inside a cluster on the administrator device.

By default, VLAN check is performed.

Example

```
# Configure VLAN check for the communication inside a cluster.
[Huawei_0.Quidway-cluster] port-tagged vlan 1
```
2.3.17 reboot member

Syntax

```
reboot member { member-num | mac-address H-H-H } [ eraseflash ]
```

View

Cluster view

Parameter

- `member-num`: Cluster member number.
- `H-H-H`: MAC address of the member device to be reset.
- `eraseflash`: Delete the configuration file when resetting the member device.

Description

Using the `reboot member` command, you can reset a specified member device on the administrator device.

The communication between the administrator device and member devices may be interrupted due to some configuration errors, the member device can be controlled via the remote control function of member device. For example, you can delete the booting configuration file and reset the member device to restore the normal communication between administrator device and member device.

When using the `reboot member` command, the user can decide to delete the configuration file or not with the `eraseflash` parameter when the member device is resetting.

Example

```
# Reset the cluster member 2.
[Huawei_0.Quidway-cluster] reboot member 2
```

2.3.18 snmp-host

Syntax

```
snmp-host ip-address
undo snmp-host
```

View

Cluster view

Parameter

- `ip-address`: IP address of the SNMP host configured for the cluster.
Description

Using **snmp-host** command, you can configure the public SNMP host for the members inside a cluster on the administrator device. Using **undo snmp-host** command, you can cancel the public SNMP host.

By default, there is no public SNMP host.

This command is used to configure the IP address of the network management site for the cluster, thereby a cluster member can send the trap information to it via the administrator device.

Example

```
# Configure the IP address of SNMP host for the cluster on the administrator device.
[Huawei_0.Quidway-cluster] snmp-host 1.0.0.9
```

### 2.3.19 tftp-server

**Syntax**

```
tftp-server ip-address
undo tftp-server
```

**View**

Cluster view

**Parameter**

`ip-address`: IP address of TFTP server configured for the cluster.

**Description**

Using **tftp-server** command, you can configure the public TFTP server for the cluster members on the administrator device. Using **undo tftp-server** command, you can cancel the public TFTP server.

By default, there is no public TFTP Server.

Assign an IP address for TFTP server of the cluster, then the member devices can access the server via the administrator device.

Example

```
# Configure IP address for TFTP server on the administrator device.
[Huawei_0.Quidway-cluster] tftp-server 1.0.0.9
```
2.3.20 timer

Syntax

```
timer interval-in-secs
undo timer
```

View

Cluster view

Parameter

`Interval-in-secs`: This parameter is to set sending time interval of the handshake packet, ranging of 1 ~ 255 seconds. By default, the value is 10 seconds.

Description

Using `timer` command, you can configure the interval of handshake packets. Using `undo timer` command, you can restore the default value of the interval.

Inside a cluster, the member devices communicate with the administrator device through transmitting handshake packets. The regular handshake can help the user monitor the states of cluster members and links.

This command can only be executed on the administrator device, which will advertise the cluster timer value to the member devices.

Example

```
# Configure to send handshake packets once every 3 seconds.
[Huawei_0.Quidway-cluster] timer 5
```
Chapter 3  Multicast MAC Address for Cluster Management Commands

3.1  Multicast MAC Address for Cluster Management Commands

3.1.1  cluster-mac

Syntax

```
cluster-mac H-H-H
```

View

Cluster view

Parameter

- **H-H-H**: MAC address of the client host, in hexadecimal notation. It is in the range of 0180-C200-0000 or 0180-C200-000A and 0180-C200-0020 to 0180-C200-002F.

Description

Use the **cluster-mac** command to configure a multicast MAC address for cluster management. You can only use this command on the management device.

When the management device is configured with a multicast MAC address, it can send multicast packets to the cluster member switches.

After the multicast MAC address is configured, the system prompts you to define the time interval for sending multicast packets if it is 0.

Example

```
# Configure the multicast MAC address of the management device as 0180-C200-0000.

[huawei_0.Quidway-cluster] cluster-mac 0180-C200-0000
```

3.1.2  cluster-mac syn-interval

Syntax

```
cluster-mac syn-interval time-interval
```

Huawei Technologies Proprietary
View

Cluster view

Parameter

\textit{time-interval}: Time interval for sending multicast messages, in minutes.

Description

Use the \texttt{cluster-mac sync-interval} command to set the time interval for sending multicast messages on the management device. You can only use this command on the management device.

If the time interval for sending multicast messages is set to 0, the management device does not send multicast messages to the cluster member switches.

Example

\begin{verbatim}
# Set the time interval for sending multicast messages to 1 minute.
[huawei_0.Quidway-cluster] cluster-mac sync-interval 1
\end{verbatim}
# Table of Contents

## Chapter 1 MSTP Configuration Commands

1.1.1 active region-configuration ................................................................. 1-1
1.1.2 check region-configuration ............................................................... 1-1
1.1.3 display stp ........................................................................................ 1-3
1.1.4 display stp region-configuration ...................................................... 1-5
1.1.5 instance ......................................................................................... 1-6
1.1.6 region-name .................................................................................. 1-6
1.1.7 reset stp ......................................................................................... 1-7
1.1.8 revision-level ................................................................................. 1-8
1.1.9 stp ................................................................................................. 1-9
1.1.10 stp bpdu-protection ..................................................................... 1-9
1.1.11 stp bridge-diameter ..................................................................... 1-10
1.1.12 stp bridge-priority ....................................................................... 1-11
1.1.13 stp edged-port .............................................................................. 1-12
1.1.14 stp cost ......................................................................................... 1-13
1.1.15 stp port priority ............................................................................ 1-14
1.1.16 stp root primary ........................................................................... 1-15
1.1.17 stp root secondary ....................................................................... 1-16
1.1.18 stp interface ............................................................................... 1-17
1.1.19 stp interface edged-port ............................................................... 1-18
1.1.20 stp interface cost ......................................................................... 1-19
1.1.21 stp interface port priority ............................................................. 1-21
1.1.22 stp interface loop-protection ....................................................... 1-22
1.1.23 stp interface mcheck ................................................................. 1-22
1.1.24 stp interface point-to-point........................................................... 1-23
1.1.25 stp interface root-protection ...................................................... 1-24
1.1.26 stp interface transit-limit ............................................................. 1-25
1.1.27 stp loop-protection ..................................................................... 1-26
1.1.28 stp max-hops ............................................................................. 1-27
1.1.29 stp mcheck ............................................................................... 1-27
1.1.30 stp mode .................................................................................... 1-28
1.1.31 stp point-to-point ....................................................................... 1-29
1.1.32 stp region-configuration ............................................................ 1-30
1.1.33 stp tc-protection ......................................................................... 1-30
1.1.34 stp root-protection ..................................................................... 1-31
1.1.35 stp timer forward-delay .............................................................. 1-32
1.1.36 stp timer hello ........................................................................... 1-33
1.1.37 stp timer max-age ............................................................................................... 1-34
1.1.38 stp transit-limit ................................................................................................. 1-35
1.1.39 vlan-mapping modulo ....................................................................................... 1-36
Chapter 1  MSTP Configuration Commands

1.1.1  active region-configuration

Syntax

active region-configuration

View

MST region view

Parameter

None

Description

Using active region-configuration command, you can activate the configurations of MST region.

This command is used for manually activate the configurations of MST region. Configuring the related parameters, especially the VLAN mapping table, of the MST region, will lead to the recalculation of spanning tree and network topology flapping. To bate such flapping, MSTP applies the configured parameters and launches recalculation of the spanning tree only when you activate the configured MST region parameters or enable MSTP.

After you entered this command, MSTP will apply the MST region parameters you configured to the system and recalculate the spanning tree.

For the related command, see instance, region-name, revision-level, vlan-mapping modulo, check region-configuration .

Example

# Manually activate MST region configurations.
[Quidway-mst-region] active region-configuration

1.1.2  check region-configuration

Syntax

check region-configuration

View

MST region view
Parameter
None

Description
Using `check region-configuration` command, you can view the configuration information (including switch region name, revision level, and VLAN mapping table) to be activated.

MSTP defines that the user must ensure the correct region configurations, especially the VLAN mapping table configuration. The switches can be configured in the same region only if their region names, VLAN mapping tables, and MSTP revision levels are configured exactly the same. The switch may not be configured in the expected region due to any slight deviation. You can use this command to display the MST region configuration information to be activated to know to which MST regions the switch belongs and check if the MST region configurations are correct.

For the related command, see `instance`, `region-name`, `revision-level`, `vlan-mapping modulo`, `active region-configuration`.

Example

```
# Display the configuration information about the region.
[Quidway-mst-region] check region-configuration
Admin. Configuration:
    Format selector :0
    Region name     :00b010000001
    Revision level  :0

    Instance   Vlans Mapped
          0       1 to 9, 11 to 4094
          16      10
```

Table 1-1 the display information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format selector</td>
<td>Factor to select protocol type prescribed in MSTP</td>
</tr>
<tr>
<td>Region name</td>
<td>Region name of MST region</td>
</tr>
<tr>
<td>Revision level</td>
<td>MSTP revision level of MST region</td>
</tr>
<tr>
<td>Instance</td>
<td>VLAN mapping table of MST region</td>
</tr>
<tr>
<td>Vlans Mapped</td>
<td></td>
</tr>
</tbody>
</table>
1.1.3 display stp

Syntax

display stp [ instance instance-id ] [ interface interface-list | slot slot-num ] [ brief ]

View

Any view

Parameter

instance-id: Specifies the spanning tree instance ID, ranging from 0 to 16, instance 0 is CIST.

interface-list: Ethernet port list, containing multiple Ethernet ports and expressed as interface-list = { { interface-type interface-num | interface-name } | to { interface-type interface-num | interface-name } } &<1-10>. For detail descriptions of interface-type, interface-num and interface-name parameters, refer to the corresponding descriptions in Port Command Manual. &<1-10> means that the preceding parameters can be entered up to 10 times.

slot slot-num: Configure to display the STP configuration of specified slot.

brief: Configure to display the state and protection type of the port only, instead of any other information.

Description

Using display stp command, you can view the state information and statistics information of the spanning tree.

The MSTP state and statistics information can help analyze and maintain the network topology and maintain the normal operation of MSTP.

If no STI ID or port list is specified, the command will display the spanning tree information of all the instances on all the ports in port number order. If the instance ID is specified, the command will display the spanning tree information of the specified instance on all the port in port number order. If only the port list is specified, the command will display the information about all the STIs on the port in port number order. If both the STI ID and port list are specified, the command will displays the spanning tree information of the specified instance on the specified port in instance ID order.

MSTP state information include:

1) Global CIST parameter: Protocol operation mode, switch priority in the CIST instance, MAC address, Hello Time, Max Age, Forward Delay, Max Hops, CIST common root, external path cost of the switch to the CIST common root, region root, internal path cost of the switch to the CIST common root, CIST root port of the switch, and whether to enable BPDU protection;
2) CIST port parameter: Port state, role, priority, path cost, designated bridge, designated port, edge port/non-edge port, whether connected to the point-to-point link, port transit limit, whether to enable Root protection, whether being a region edge port, Hello Time, Max Age, Forward Delay, Message-age time, and Remaining-hops;

3) Global MSTIs parameter: MSTI instance ID, bridge priority of the instance, region root, internal path cost, MSTI root port, and MASTER bridge;

4) MSTIs port parameter: Port state, role, priority, path cost, designated bridge, and Remaining Hops.

Statistics information: Count of TCN, CONFIG BPDU, RST, and MST BPDU transmitted/received via the port.

For the related command, see `reset stp`.

**Example**

# Display the state and statistics information about the spanning tree.

```bash
<Quidway> display stp instance 0 interface ethernet0/1 to ethernet0/10 brief
```

<table>
<thead>
<tr>
<th>MSTID</th>
<th>Port</th>
<th>STP State</th>
<th>Guard Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>ethernet0/1</td>
<td>DOWN</td>
<td>none</td>
</tr>
<tr>
<td>0</td>
<td>ethernet0/2</td>
<td>DOWN</td>
<td>none</td>
</tr>
<tr>
<td>0</td>
<td>ethernet0/3</td>
<td>DOWN</td>
<td>none</td>
</tr>
<tr>
<td>0</td>
<td>ethernet0/4</td>
<td>DOWN</td>
<td>none</td>
</tr>
<tr>
<td>0</td>
<td>ethernet0/5</td>
<td>DOWN</td>
<td>none</td>
</tr>
<tr>
<td>0</td>
<td>ethernet0/6</td>
<td>DOWN</td>
<td>none</td>
</tr>
<tr>
<td>0</td>
<td>ethernet0/7</td>
<td>DOWN</td>
<td>none</td>
</tr>
<tr>
<td>0</td>
<td>ethernet0/8</td>
<td>DOWN</td>
<td>none</td>
</tr>
<tr>
<td>0</td>
<td>ethernet0/9</td>
<td>DOWN</td>
<td>none</td>
</tr>
<tr>
<td>0</td>
<td>ethernet0/10</td>
<td>DOWN</td>
<td>none</td>
</tr>
</tbody>
</table>

The above information indicates that the MSTIDs of the ethernet0/1 through ethernet0/10 are all 0, that is, all these ports belong to CIST.

**Table 1-2 the display Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSTID</td>
<td>MST instance ID of the port</td>
</tr>
<tr>
<td>Port</td>
<td>Port number</td>
</tr>
<tr>
<td>STP State</td>
<td>STP State of the port, which can be up or down.</td>
</tr>
<tr>
<td>Guard Type</td>
<td>Guard Type of the port, which can be</td>
</tr>
</tbody>
</table>
1.1.4 display stp region-configuration

Syntax

display stp region-configuration

View

Any view

Parameter

None

Description

Using `display stp region-configuration` command, you can view the effective MST region configurations.

MST region configuration information includes: region name, region revision level, and associations between VLANs and STIs. All these configurations together determine to which MST region a switch belongs.

For the related command, see `stp region-configuration`.

Example

# Display the MST region configuration information.
<Quidway> display stp region-configuration
Oper. Configuration:
    Format selector :0
    Region name :huawei
    Revision level :0

    Instance Vlans Mapped
    0 21 to 4094
    1 1 to 10
    2 11 to 20

Table 1-3 the display Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format selector</td>
<td>Factor to select protocol type prescribed in MSTP</td>
</tr>
<tr>
<td>Region name</td>
<td>Region name of MST region</td>
</tr>
<tr>
<td>Revision level</td>
<td>MSTP revision level of MST region</td>
</tr>
<tr>
<td>Instance Vlans Mapped</td>
<td>VLAN mapping table of MST region</td>
</tr>
</tbody>
</table>
1.1.5 instance

Syntax

```
instance instance-id vlan vlan-list
undo instance instance-id [v lan vlan-list]
```

View

```
MST region view
```

Parameter

- **instance-id**: Specifies the spanning tree instance ID, ranging from 0 to 16, instance 0 is CIST.
- **vlan-list**: Specifies the VLAN list and expressed as `vlan-list = {vlan-id [to vlan-id]}&<1-10>`. VLAN ID ranges from 1 to 4094. &<1-10> means that the preceding parameters can be entered up to 10 times. The switch may support VLAN 4095, 4096 others, however, they can only be mapped to CIST (Instance 0).

Description

Using **instance** command, you can map the specified VLAN list to the specified STI. Using **undo instance** command, you can cancel the specified VLAN list from the specified STI, the removed VLAN will then be mapped to the CIST (i.e., the Instance 0).

If no VLAN is specified in the **undo** command, all the VLANs associated with the specified STI will be mapped to CIST.

By default, all the VLANs are mapped to CIST, i.e., the Instance 0.

MSTP describes the association between VLANs and STIs with the VLAN mapping table. You can use this command to configure this table. Every VLAN can be mapped to an STI as per your configuration.

A VLAN cannot be mapped to different instances at the same time. The latter configured association will replace the former one.

For the related command, see **region-name**, **revision-level**, **check region-configuration**, **vlan-mapping modulo**, **active region-configuration**.

Example

```
# Map VLAN 2 to STI 1.
[Quidway-mst-region] instance 1 vlan 2
```

1.1.6 region-name

Syntax

```
region-name name
```
undo region-name

**View**

MST region view

**Parameter**

*name*: Specifies the MST region name of the switch with a character string not exceeding 32 bytes.

**Description**

Using `region-name` command, you can configure the MST region name of a switch. Using `undo region-name` command, you can restore the default MST region name. By default, the MST region name of the switch is the first MAC address in hexadecimal notation.

The switch region name, together with VLAN mapping table of the MST region and MSTP revision level, is used for determining the region to which the switch belongs.

For the related command, see `instance, revision-level, check region-configuration, vlan-mapping modulo, active region-configuration`.

**Example**

# Set the MST region name of the switch as huawei.

![Quidway-mst-region] region-name huawei

### 1.1.7 reset stp

**Syntax**

`reset stp [ interface interface-list ]`

**View**

User view

**Parameter**

*interface-list*: Ethernet port list, containing multiple Ethernet ports and expressed as

```
interface_list = { { interface_type interface_num | interface_name } [ to { interface_type interface_num | interface_name } ] }&<1-10>. For detail descriptions of `interface_type, interface_num` and `interface_name` parameters, refer to the corresponding descriptions in Port Command Manual. &<1-10> means that the preceding parameters can be entered up to 10 times.
```

**Description**

Using `reset stp` command, you can reset the spanning tree statistics information.
The spanning tree statistics information includes TCN, Config BPDU, RST, and MST BPDU, received and transmitted on the port. Among them, STP BPDU and TCN BPDU are counted on CIST.

When the spanning tree ID and port list are specified, the command clears the statistics information of the specified spanning tree on the specified port. If no port is specified, the command clears the statistics information of the specified spanning tree on all the ports. If no spanning tree is specified, the command clears the statistics information of all the spanning trees.

For the related command, see `display stp`.

**Example**

```
# Clear the statistics information on the ports from ethernet0/1 through ethernet0/3.
<Quidway> reset stp interface ethernet0/1 to ethernet0/3
```

### 1.1.8 revision-level

**Syntax**

```
revision-level level
undo revision-level
```

**View**

MST region view

**Parameter**

`level`: Specifies the MSTP revision level, ranging from 0 to 65535. By default, MSTP revision level takes 0.

**Description**

Using `revision-level` command, you can configure MSTP revision level of the switch. Using `undo revision-level` command, you can restore the default revision-level.

MSTP revision level, together with region name and VLAN mapping table, is used for determining the MST region to which the switch belongs.

For the related command, see `instance`, `region-name`, `check region-configuration`, `vlan-mapping modulo` and `active region-configuration`.

**Example**

```
# Set the MSTP revision level of the switch MST region to 5.
[Quidway-mst-region] revision-level 5
```
1.1.9 stp

Syntax

stp { enable | disable }
undo stp

View

System view, Ethernet port view

Parameter

enable: Enables global or port MSTP.
disable: Disables global or port MSTP.

Description

Using stp command, you can enable or disable MSTP on a device or a port. Using undo stp command, you can restore the default MSTP state on a device or a port.

By default, MSTP is disabled on the switch.

After MSTP is enabled, the switch determines to run MSTP in STP-compatible mode or MSTP mode per your configurations. The switch serves as a transparent bridge after MSTP is disabled.

After MSTP is enabled, it will dynamically maintain the spanning tree state of the corresponding VLAN according to the received configuration BPDU until it is disabled.

For the related command, see stp mode, stp interface.

Example

# Enable MSTP globally.
[Quidway] stp enable

# Disable MSTP on ethernet0/1.
[Quidway-Ethernet0/1] stp disable

1.1.10 stp bpdu-protection

Syntax

stp bpdu-protection
undo stp bpdu-protection

View

System view
**Parameter**

None

**Description**

Using **stp bpdu-protection** command, you can enable the BPDU protection on the switch. Using **undo stp bpdu-protection** command, you can restore the default state of BPDU protection.

By default, BPDU protection is disabled.

Generally, the access ports of the access layer devices are directly connected to user terminals (such as PC) or file servers. In this case, the access ports are set to edge ports to implement fast state transition. However, when such access ports receive configuration BPDU, the system will automatically set them to non-edge ports and recalculate the spanning tree, which makes the network topology flap. These ports will not receive any STP configuration BPDU in normal cases. Anyway, if someone maliciously attacks the switch with fake configuration BPDU, the network will flap.

MSTP provides BPDU protection function to avoid such attack: After configured with BPDU protection, the switch will disable the edge port through MSTP, which receives a BPDU, and notify the network manager at same time. These ports can be resumed by the network manager only.

**Example**

```
# Enable BPDU protection on the switch.
[Quidway] stp bpdu-protection
```

### 1.1.11 stp bridge-diameter

**Syntax**

```
stp bridge-diameter bridgenum
undo stp bridge-diameter
```

**View**

System view

**Parameter**

`bridgenum`: Ranges from 2 to 7 and defaults to 7.

**Description**

Using **stp bridge-diameter** command, you can configure the switching network diameter. Using **undo stp bridge-diameter** command, you can restore the default network diameter.
The network diameter refers to the maximum count of switches on the path between any two terminal devices.

The definition of network diameter: Maximum count of switches between the farthest communication ends.

**stp bridge-diameter** command configures the switching network diameter and determines the three time parameters of MSTP accordingly. This configuration takes effect on CIST only but makes no sense for MSTI.

The spanning tree convergence can be speeded up, when Hello Time, Forward Delay, and Max Age are well configured. These parameters are related to the network scale.

You can configure the network scale to get the time parameters. Upon the user-configured bridge-diameter parameter, MSTP will automatically set Hello Time, Forward Delay, and Max Age to moderate values. When bridge-diameter defaults to 7, the time parameters also take their respective default values.

For the related command, see **stp timer forward-delay**, **stp timer hello**, **stp timer max-age**.

**Example**

```
# Set the diameter of the switching network to 5.
[Quidway] stp bridge-diameter 5
```

**1.1.12 stp bridge-priority**

**Syntax**

```
stp [ instance instance-id ] bridge-priority priority
undo stp [ instance instance-id ] bridge-priority
```

**View**

System view

**Parameter**

- **instance-id**: Specifies the spanning tree instance ID, ranging from 0 to 16, instance 0 is CIST.
- **priority**: Specifies the switch priority, ranging from 0 to 61440 with a step length of 4096. That is, 16 priorities are available for the switch including 0, 4096, 8192, etc. By default, the switch priority is 32768.

**Description**

Using **stp bridge-priority** command, you can configure the bridge priority in the specified STI. Using **undo stp bridge-priority** command, you can restore the default value of bridge priority .
The switch priority takes part in the spanning tree calculation. It is configured separately for every STI. Different STIs can be configured with different priorities.

If specifying the instance ID as 0, the command can configure the CIST priority. If user doesn’t input parameter “instance instance-id” when configuring switch, the configuration will only be effective on CIST.

Example

# Set the bridge priority of the switch in STI 1 to 4096.
[Quidway] stp instance 1 bridge-priority 4096

1.1.13 stp edged-port

Syntax

stp edged-port { enable | disable }
undo stp edged-port

View

Ethernet port view

Parameter

enable: Configure the current port as an edge port.
disable: Configure the current port as a non-edge port.

Description

Using stp edged-port enable command, you can configure the current Ethernet port as an edge port. Using stp edged-port disable command, you can configure the current Ethernet port as a non-edge port. Using undo stp edged-port command, you can restore the default state, i.e., non-edge port.

By default, all the switch ports are configured as non-edge port.

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 configure it as a non-edge port. The stp edged-port enable command is used for configuring the port as an edge port.

A port is considered as an edge port when it is directly connected to the user terminal, instead of any other switches or shared network segments. The edge port will not cause loop upon network topology changes. Accordingly, you can configure a port as an edge port, so that it can transit to forwarding state fast. For this purpose, please configure the Ethernet port directly connected to the user terminal as an edge port.
Because the edge port is not connected to any other switches, it will not receive the configuration BPDUUs from them. Before BPDU PROTECTION is enabled on the switch, the port received a BPDU runs as a non-edge port, even if it is configured as edge port.

For the related command, see `stp interface edged-port`.

**Example**

```
# Configure ethernet0/1 as an edge port.
[Quidway-Ethernet0/1] stp edged-port disable
```

### 1.1.14 stp cost

**Syntax**

```
stp [ instance instance-id ] cost cost
undo stp [ instance instance-id ] cost
```

**View**

Ethernet port view

**Parameter**

- `instance-id`: Specifies the spanning tree instance ID, ranging from 0 to 16, instance 0 is CIST.
- `cost cost`: Specifies the port path cost, ranging from 1 to 200000.

**Description**

Using `stp cost` command, you can configure the port path cost on the specified STI for the current port. Using `undo stp cost` command, you can restore the path cost on the specified STI.

By default, the path costs of a port on different STIs take the values associated with the port speeds. For more description, refer to the table offered in the configuration guideline of the `stp interface cost` command.

You may specify the `instance-id` parameter as 0 to configure CIST path cost of the port. The path cost has effect on the port role selection. A port can be configured with different path costs on different MSTIs. Thus the traffic from different VLANs can run over different physical links, thereby implementing the VLAN-based load-balancing. MSTP will recalculate the port role and transit its state, upon the port path cost changes.

If user doesn’t input parameter "`instance instance-id`" when configuring switch, the configuration will only be effective on CIST.

The default values of the path cost varies with the different port speeds, as described in the following table.
### Table 1-4 Cost corresponding to the port speed

<table>
<thead>
<tr>
<th>Link speed</th>
<th>Recommended value</th>
<th>Recommended value range</th>
<th>Value range</th>
</tr>
</thead>
<tbody>
<tr>
<td>10Mbps</td>
<td>2,000</td>
<td>200- 20000</td>
<td>1-200000</td>
</tr>
<tr>
<td>100Mbps</td>
<td>200</td>
<td>20-2000</td>
<td>1-200000</td>
</tr>
<tr>
<td>1Gbps</td>
<td>20</td>
<td>2-200</td>
<td>1-200000</td>
</tr>
<tr>
<td>10G/s</td>
<td>2</td>
<td>2-20</td>
<td>1-200000</td>
</tr>
<tr>
<td>Above 10G/s</td>
<td>1</td>
<td>1-2</td>
<td>1-200000</td>
</tr>
</tbody>
</table>

For the related command, see `stp interface cost`.

**Example**

```
# Set the path cost of ethernet0/3 on STI 2 to 200.
[Quidway-Ethernet0/3] stp instance 2 cost 200
```

### 1.1.15 stp port priority

**Syntax**

```
stp [ instance instance-id ] port priority priority
undo stp [ instance instance-id ] port priority
```

**View**

Ethernet port view

**Parameter**

- `instance-id`: Specifies the spanning tree instance ID, ranging from 0 to 16, instance 0 is CIST.
- `port priority priority`: Specifies the port priority, ranging from 0 to 240, with a step length of 16, e.g., 0, 16, and 32. By default, the priorities of a port on the STIs are 128.

**Description**

Using `stp port priority` command, you can configure the priority of a port on a specified STI. Using `undo stp port priority` command, you can restore the default priority of the port on the specified STI.

You may specify the `instance-id` parameter as 0 to configure CIST priority of the port. The port priority has effect on the port role selection. A port can be configured with different priorities on different MSTIs. Thus the traffic from different VLANs can run over different physical links, thereby implementing the VLAN-based load-balancing. MSTP will recalculate the port role and transit its state, upon the port priority changes.
If user doesn’t input parameter “instance instance-id” when configuring switch, the configuration will only be effective on CIST.

For the related command, see stp interface port priority.

Example

# Set the priority of ethernet0/3 on STI 2 to 16.
[Quidway-Ethernet0/3] stp instance 2 port priority 16

1.1.16 stp root primary

Syntax

stp [ instance instance-id ] root primary [ bridge-diameter bridgenum ] [ hello-time centi-seconds ]
undo stp [ instance instance-id ] root

View

System view

Parameter

instance-id: Specifies the spanning tree instance ID, ranging from 0 to 16, instance 0 is CIST.
root primary: Configure the current switch as the primary root of the designated STI.
bridge-diameter bridgenum: Specify the network diameter of the spanning tree, ranging from 2 to 7.
hello-time centi-seconds: Specifies the Hello Time of the spanning tree, ranging from 100 to 1000 and measured in centiseconds.

Description

Using stp root primary command, you can configure the current switch as the primary root of the designated STI. Using undo stp root command, you can cancel the current switch for the primary root of the designated STI. If user doesn’t input parameter “instance instance-id” when configuring switch, the configuration will only be effective on CIST.

By default, the switch does not server as a root bridge.

You can configure a root bridge for every STI without concerning the switch priority. When configuring the root bridge, you may also specify the network diameter of the designated switching network, so that the switch will calculate and get three time parameter values (Hello time, Forward Delay and Max Age). The Hello time got in this way may not be as good as expected. You can specify the hello-time centi-seconds.
parameter to overwrite it. Normally, you are recommended to set the network diameter to get the other two time parameter of the switch accordingly.

⚠️ Caution:

- In a switching network, you can configure only one root bridge for each STI and one or more secondary switches. Do not configure more than one root bridge for an STI at the same time, otherwise, the calculation result will be unpredictable.
- After a switch is configured as primary root switch or secondary root switch, user can't modify the bridge priority of the switch.

Example

# Designate the current switch as the root bridge of STI 1 and specifies the diameter of the switching network as 4 and the Hello Time as 500 centiseconds.

[Quidway] stp instance 1 root primary bridge-diameter 4 hello-time 500

1.1.17 stp root secondary

Syntax

stp [ instance instance-id ] root secondary [ bridge-diameter bridgenum ]
[ hello-time centi-seconds ]
undo stp [ instance instance-id ] root

View

System view

Parameter

instance-id: Specifies the spanning tree instance ID, ranging from 0 to 16, instance 0 is CIST.
root secondary: Configure the current switch as the secondary root of the designated STI.
bridge-diameter bridgenum: Specify the network diameter of the spanning tree, ranging from 2 to 7.
hello-time centi-seconds: Specify the Hello Time of the spanning tree, ranging from 100 to 1000 and measured in centiseconds.
**Description**

Using **stp root secondary** command, you can configure the current switch as the secondary root bridge of a specified STI. Using **undo stp root** command, you can cancel the current switch for the secondary root bridge of a specified STI. If user doesn't input parameter “**instance instance-id**” when configuring switch, the configuration will only be effective on CIST.

By default, the switch does not serve as a secondary root bridge.

You can configure one or more secondary root bridges in an STI. If the primary root is down or powered off, the secondary root will take its place. Among several secondary root bridges, the one with the smallest MAC address takes the place of the failed primary root.

When configuring the secondary root bridge, you may also specify the switching network diameter and the Hello Time of the switch, so that the other two parameters, Forward Delay and Max Age, of the switch can be determined. To configure the current switch as the root bridge of CIST, simply specify **instance-id** as 0. You can configure only one root bridge for an STI and one or more secondary root bridges for it.

After a switch is configured as primary root switch or secondary root switch, user can’t modify the bridge priority of the switch.

**Example**

```plaintext
# Configure the current switch as the secondary root bridge of STI 4 and specify the diameter of the switching network as 5 and the Hello Time of the switch as 300 centiseconds.

[Quidway] stp instance 4 root primary bridge-diameter 5 hello-time 300
```

**1.1.18 stp interface**

**Syntax**

```plaintext
stp interface interface-list { enable | disable }
```

**View**

System view

**Parameter**

`interface-list`: Ethernet port list, containing multiple Ethernet ports and expressed as `interface_list = { { interface_type interface_num | interface_name } [ to { interface_type interface_num | interface_name } ] }<1-10>`. For detail descriptions of `interface_type`, `interface_num` and `interface_name` parameters, refer to the corresponding descriptions in Port Command Manual. `<1-10>` means that the preceding parameters can be entered up to 10 times.
enable: Enables MSTP on the port.
disable: Disables MSTP on the port.

Description

Using stp interface command, you can enable/disable MSTP on a switch port in system view.

By default, if MSTP is enabled globally, it is enabled on every port; if MSTP is disabled globally, it is also disabled on every port.

When MSTP is disabled, the corresponding port stays in forwarding state and does not take part in any STI calculation.

⚠️ Caution:

Loop may be generated, if you disable MSTP on the port.

For the related command, see stp mode, stp.

Example

# Enable MSTP on ethernet0/1 in system view.
[Quidway] stp interface ethernet0/1 enable

1.1.19 stp interface edged-port

Syntax

stp interface interface-list edged-port {enable | disable }
undo stp interface interface-list edged-port

View

System view

Parameter

interface-list: Ethernet port list, containing multiple Ethernet ports and expressed as interface_list = { { interface_type interface_num | interface_name } [ to { interface_type interface_num | interface_name } ] }&<1-10>. For detail descriptions of interface_type, interface_num and interface_name parameters, refer to the corresponding descriptions in Port Command Manual. &<1-10> means that the preceding parameters can be entered up to 10 times.

enable: Configure the current port as an edge port.
**disable**: Configure the current port as a non-edge port.

**Description**

Using `stp interface edged-port enable` command, you can configure a port as an edge port in system view. Using `stp interface edged-port disable` command, you can configure a port as a non-edge port in system view. Using `undo stp interface edged-port` command, you can restore the non-edge port, as defaulted.

By default, all the switch ports are configured as non-edge port.

If the current Ethernet port is connected to other switch, you can use the `stp interface edged-port disable` or `no stp interface edged-port` command to configure it as a non-edge port. The `stp interface edged-port enable` command is used for configuring the port as an edge port.

A port is considered as an edge port when it is directly connected to the user terminal, instead of any other switches or shared network segments. The edge port will not cause loop upon network topology changes. Accordingly, you can configure a port as an edge port, so that it can transit to forwarding state fast. For this purpose, please configure the Ethernet port directly connected to the user terminal as an edge port.

Because the edge port is not connected to any other switches, it will not receive the configuration BPDUs from them. Before BPDU PROTECTION is enabled on the switch, the port received a BPDU runs as a non-edge port, even if it is configured as edge port.

For the related command, see `stp edged-port`.

**Example**

```
# Configure ethernet0/3 as an edge port in system view.
[Quidway] stp interface ethernet0/3 edged-port enable
```

### 1.1.20 stp interface cost

**Syntax**

```
stp interface interface-list [ instance instance-id ] cost cost
undo stp interface interface-list [ instance instance-id ] cost
```

**View**

System view

**Parameter**

- `interface-list`: Ethernet port list, containing multiple Ethernet ports and expressed as `interface_list = { { interface_type interface_num | interface_name } { to { interface_type interface_num | interface_name } } }&<1-10>`. For detail descriptions of `interface_type`, `interface_num` and `interface_name` parameters, refer to the corresponding descriptions...
instance-id: Specifies the spanning tree instance ID, ranging from 0 to 16, instance 0 is CIST.

cost cost: Specifies the path cost of the port, ranging from 1 to 200000.

Description

Using `stp interface cost` command, you can configure the path cost of the specified port on the specified STI in system view. Using `undo stp interface cost` command, you can restore the path cost to default value. If user doesn't input parameter “instance instance-id” when configuring switch, the configuration will only be effective on CIST.

By default, the path cost of the port on every STI is associated with the port speed. For details, refer to the table in the configuration guideline.

You may specify the `instance-id` parameter as 0 to configure CIST path cost of the port. The path cost has effect on the port role selection. A port can be configured with different path costs on different MSTIs. Thus the traffic from different VLANs can run over different physical links, thereby implementing the VLAN-based load-balancing. MSTP will recalculate the port role and transit its state, upon the port path cost changes.

The default values of the path cost varies with the different port speeds, as described in the following table.

<table>
<thead>
<tr>
<th>Link speed</th>
<th>Recommended value</th>
<th>Recommended value range</th>
<th>Value range</th>
</tr>
</thead>
<tbody>
<tr>
<td>10Mbps</td>
<td>2,000</td>
<td>200-20000</td>
<td>1-200000</td>
</tr>
<tr>
<td>100Mbps</td>
<td>200</td>
<td>20-2000</td>
<td>1-200000</td>
</tr>
<tr>
<td>1Gbps</td>
<td>20</td>
<td>2-200</td>
<td>1-200000</td>
</tr>
<tr>
<td>10G/s</td>
<td>2</td>
<td>2-20</td>
<td>1-200000</td>
</tr>
<tr>
<td>Above 10G/s</td>
<td>1</td>
<td>1-2</td>
<td>1-200000</td>
</tr>
</tbody>
</table>

For the related command, see `stp cost`.

Example

# Set the path cost of ethernet0/3 on STI 2 to 400 in system view.

[Quidway] stp interface ethernet0/3 instance 2 cost 400
### 1.1.21 `stp interface port priority`

**Syntax**

```
stp interface interface-list [ instance instance-id ] port priority priority
undo stp interface interface-list [ instance instance-id ] port priority
```

**View**

System view

**Parameter**

- `interface-list`: Ethernet port list, containing multiple Ethernet ports and expressed as `interface_list = { { interface_type interface_num | interface_name } [ to { interface_type interface_num | interface_name } ] }&<1-10>`. For detail descriptions of `interface_type`, `interface_num` and `interface_name` parameters, refer to the corresponding descriptions in Port Command Manual. `&<1-10>` means that the preceding parameters can be entered up to 10 times.
- `instance-id`: Specifies the spanning tree instance ID, ranging from 0 to 16, instance 0 is CIST.
- `port priority priority`: Specifies the port priority, ranging from 0 to 240 with a step length of 16, e.g., 0, 16 and 32. By default, the port has a priority of 128 on every STI.

**Description**

Using `stp interface port priority` command, you can configure the priority of the specified port on the specified STI in system view. Using `undo stp interface port priority` command, you can restore the default priority. If user doesn’t input parameter `“instance instance-id”` when configuring switch, the configuration will only be effective on CIST.

You may specify the `instance-id` parameter as 0 to configure CIST priority of the port. The port priority has effect on the port role selection. A port can be configured with different priorities on different MSTIs. Thus the traffic from different VLANs can run over different physical links, thereby implementing the VLAN-based load-balancing. MSTP will recalculate the port role and transit its state, upon the port priority changes.

For the related command, see `stp port priority`.

**Example**

```
# Set the priority of ethernet0/3 on STI 2 to 16 in system view.
[Quidway] stp interface ethernet0/3 instance 2 port priority 16
```
1.1.22 stp interface loop-protection

Syntax

```
stp interface interface-list loop-protection
undo stp interface interface-list loop-protection
```

View

System view

Parameter

- `interface-list`: Ethernet port list, containing multiple Ethernet ports and expressed as `interface_list = {{ interface_type interface_num | interface_name } [ to { interface_type interface_num | interface_name } ]}&<1-10>`. For detail descriptions of `interface_type`, `interface_num` and `interface_name` parameters, refer to the corresponding descriptions in Port Command Manual. &<1-10> means that the preceding parameters can be entered up to 10 times.

Description

Using `stp interface loop-protection` command, you can enable loop protection on the switch in system view. Using `undo stp interface loop-protection` command, you can restore the default loop protection state.

By default, loop protection is disabled.

For the related command, see `stp loop-protection`.

Example

```
# Enable loop protection on the ethernet0/1.
[Quidway] stp interface ethernet0/1 loop-protection
```

1.1.23 stp interface mcheck

Syntax

```
stp interface interface-list mcheck
```

View

System view

Parameter

- `interface-list`: Ethernet port list, containing multiple Ethernet ports and expressed as `interface_list = {{ interface_type interface_num | interface_name } [ to { interface_type interface_num | interface_name } ]}&<1-10>`. For detail descriptions of `interface_type`, `interface_num` and `interface_name` parameters, refer to the corresponding descriptions in Port Command Manual. &<1-10> means that the preceding parameters can be entered up to 10 times.
in Port Command Manual. &<1-10> means that the preceding parameters can be entered up to 10 times.

Description

Using **stp interface mcheck** command, you can perform mcheck operation on the port in system view.

If a port of an MSTP switch on a switching network has ever been connected to an STP switch, the port will automatically transit to operate in STP-compatible mode. However, when the STP switch is removed, the port stays in STP-compatible mode and cannot automatically transit back to MSTP mode. In this case, you can perform mCheck operation to transit the port to MSTP mode by force.

For the related command, see **stp mcheck, stp mode**.

Example

```bash
# Set mcheck parameter of ethernet0/3 in system view.
[Quidway] stp interface ethernet0/3 mcheck
```

1.1.24 **stp interface point-to-point**

Syntax

```ini
stp interface interface-list point-to-point { force-true | force-false | auto }
undo stp interface interface-list point-to-point
```

View

System view

Parameter

- **interface-list**: Ethernet port list, containing multiple Ethernet ports and expressed as
  
  `interface_list = { { interface_type interface_num | interface_name } [ to { interface_type interface_num | interface_name } ] }&<1-10>`.
  
  For detail descriptions of `interface_type`, `interface_num` and `interface_name` parameters, refer to the corresponding descriptions in Port Command Manual. &<1-10> means that the preceding parameters can be entered up to 10 times.

- **force-true**: Indicates the Ethernet port connected to a point-to-point link.

- **force-false**: Indicates the Ethernet port not connected to a point-to-point link.

- **auto**: Configure to automatically check if the link to the Ethernet port is a point-to-point link.
Description

Using `stp interface point-to-point` command, you can configure a port (not) to be connected to a point-to-point link in system view. Using `undo stp interface point-to-point` command, you can restore the default state of the link to the Ethernet port.

By default, the parameter defaults to auto, that is, MSTP checks if the link to the Ethernet port is a point-to-point link.

The port state can’t be rapidly transited if the port doesn’t connected with the point-to-point link.

The master ports of the link aggregation and the ports operating in full-duplex mode are connected to the point-to-point link. You are recommended to keep the default settings and let MSTP detect the link state automatically.

This configuration takes effect on the CIST and all the MSTIs. The settings of a port whether to connect the point-to-point link will be applied to all the STIs where the port belongs. Note that a temporary loop may be redistributed if you configure a port not physically connected with the point-to-point link as connected to such a link by force.

For the related command, see `stp point-to-point`.

Example

```
# Configure ethernet0/3 to be connected to the point-to-point link in system view.
[Quidway] stp interface ethernet0/3 point-to-point force-true
```

1.1.25 `stp interface root-protection`

Syntax

```
stp interface interface-list root-protection
undo stp interface interface-list root-protection
```

View

System view

Parameter

`interface-list`: Ethernet port list, containing multiple Ethernet ports and expressed as

```
interface_list = { { interface_type interface_num | interface_name } [ to { interface_type interface_num | interface_name } ] } &<1-10>.
```

For detail descriptions of `interface_type`, `interface_num` and `interface_name` parameters, refer to the corresponding descriptions in Port Command Manual. &<1-10> means that the preceding parameters can be entered up to 10 times.
Description

Using `stp interface root-protection` command, you can enable Root protection on the switch in system view. Using `undo stp interface root-protection` command, you can restore the default Root protection state.

By default, Root protection is disabled.

In case of configuration error or malicious attack, the legal primary root may receive the BPDU with a higher priority and then loose its place, which causes network topology change errors. Due to the illegal change, the traffic supposed to travel over the high-speed link may be pulled to the low-speed link and congestion will occur on the network.

Root protection function is used against such problem. The port configured with Root protection only plays a role of designated port on every instance. Whenever such port receives a higher-priority BPDU, that is, it is about to turn into non-designated port, it will be set to listening state and not forward packets any more (as if the link to the port is disconnected). If the port has not received any higher-priority BPDU for a certain period of time thereafter, it will resume the normal state.

For the related command, see `stp root-protection`.

Example

```
# Enable Root protection on the ethernet0/1.
[Quidway] stp interface ethernet0/1 root-protection
```

1.1.26 `stp interface transit-limit`

Syntax

```
stp interface interface-list transit-limit packetnum
undo stp interface interface-list transit-limit
```

View

System view

Parameter

- `interface-list`: Ethernet port list, containing multiple Ethernet ports and expressed as `interface_list = { { interface_type interface_num | interface_name } [ to { interface_type interface_num | interface_name } ] }&<1-10>`. For detail descriptions of `interface_type`, `interface_num` and `interface_name` parameters, refer to the corresponding descriptions in Port Command Manual. &<1-10> means that the preceding parameters can be entered up to 10 times.
packetnum: Specifies the amount limit to the transmitted packets, ranging from 1 to 255 (expressed as a counter value without any units). By default, the transmission limit on every port is 3.

**Description**

Using **stp interface transit-limit** command, you can configure an amount limit to the configuration BPDU transmitted via a port during the Hello Time in system view. Using **undo stp interface transit-limit** command, you can restore the default limit in system view.

The larger the value is, the more packets can be transmitted in a time unit, yet the more switch resources will be occupied. With a moderate value, the amount of the BPDU transmitted during Hello Time via every port can be limited and MSTP will not occupy too many bandwidth resources when the network topology flaps.

For the related command, see **stp transit-limit**.

**Example**

```
# Set a limit of 5 to the packets transmitted via ethernet0/3 in system view.
[Quidway] stp interface ethernet0/3 transit-limit 5
```

### 1.1.27 stp loop-protection

**Syntax**

```
stp loop-protection
undo stp loop-protection
```

**View**

Ethernet port view

**Parameter**

None

**Description**

Using **stp loop-protection** command, you can enable loop protection function. Using **undo stp loop-protection** command, you can restore the restore setting.

By default, the loop protection function is not enabled.

**Example**

```
# Enable loop protection function in ethernet0/1.
[Quidway-Ethernet0/1] stp loop-protection
```
1.1.28  stp max-hops

Syntax

stp max-hops hop
undo stp max-hops

View

System view

Parameter

hop: Specifies the max hops, ranging from 1 to 40. By default, MST region Max Hops is 20.

Description

Using stp max-hops command, you can configure the Max Hops of an MST region. Using undo stp max-hops command, you can restore the default Max Hops.

On CIST and MSTIs, the Max Hops configured on the region root determines the max switching network diameter supported by the local MST region. As the BPDU traveling from the spanning tree root, each time when it is forwarded by a switch, the max hops will be reduced by 1. The switch discards the configuration BPDU with 0 hops left, thereby limiting the network scale inside the region. If the current switch is a CIST root bridge or MSTI root bridge in an MST region, the Max Hops configured on it will be the network diameter of the spanning tree to limit its scale in the local MST region. The Max Hops configured on the root bridge in an MST region will be adopted by other switches in the same region.

Example

# Set the Max Hops of an MST region to 35.
[Quidway] stp max-hops 35

1.1.29  stp mcheck

Syntax

stp mcheck

View

Ethernet port view

Parameter

None
Description

Using **stp mcheck** command, you can perform mcheck on the current port. If a port of an MSTP switch on a switching network has ever been connected to an STP switch, the port will automatically transit to operate in STP-compatible mode. However, when the STP switch is removed, the port stays in STP-compatible mode and cannot automatically transit back to MSTP mode. In this case, you can perform mCheck operation to transit the port to MSTP mode by force.

For the related command, see **stp mode, stp interface mcheck**.

Example

```
# Set mcheck parameter for ethernet0/1.
[Quidway-ethernet0/1] stp mcheck
```

### 1.1.30 stp mode

**Syntax**

```
stp mode { stp | rstp | mstp }
undo stp mode
```

**View**

System view

**Parameter**

- **stp**: Specifies to run switch in STP compatible mode.
- **rstp**: Specifies to run switch in RSTP mode.
- **mstp**: Specifies to run switch in MSTP mode.

**Description**

Using **stp mode** command, you can configure the Switch running mode. Using **undo stp mode** command, you can restore the default Switch running mode.

By default, the value is **rstp**.

This command can be used for specifying the current Ethernet switch to run the RSTP in RSTP mode or in STP compatible mode.

For the related command, see **stp, stp mcheck**.

**Example**

```
# Set RSTP to work in STP compatible mode.
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] stp mode stp
```
1.1.31 stp point-to-point

Syntax

```plaintext
stp point-to-point { force-true | force-false | auto }
undo stp point-to-point
```

View

Ethernet port view

Parameter

- **force-true**: Indicates the Ethernet port connected to a point-to-point link.
- **force-false**: Indicates the Ethernet port not connected to a point-to-point link.
- **auto**: Configure to automatically check if the link to the Ethernet port is a point-to-point link.

Description

Using `stp point-to-point` command, you can configure the current Ethernet port (not) to connect with point-to-point link. Using `undo stp point-to-point` command, you can configure the link state to the default state in which MSTP automatically detects if the link to the Ethernet port is point-to-point link.

By default, switch adopts **auto** mode.

The port state can’t be rapidly transited if the port doesn’t connected with the point-to-point link.

The master ports of the link aggregation and the ports operating in full-duplex mode are connected to the point-to-point link. You are recommended to keep the default settings and let MSTP detect the link state automatically.

This configuration takes effect on the CIST and all the MSTIs. The settings of a port whether to connect the point-to-point link will be applied to all the STIs where the port belongs. Note that a temporary loop may be redistributed if you configure a port not physically connected with the point-to-point link as connected to such a link by force.

For the related command, see `stp interface point-to-point`.

Example

```plaintext
# Configure ethernet0/3 to be connected to the point-to-point link.
[Quidway-Ethernet0/3] stp point-to-point force-true
```
1.1.32 stp region-configuration

Syntax

stp region-configuration
undo stp region-configuration

View

System view

Parameter

None

Description

Using **stp region-configuration** command, you can enter MST region view. Using **undo stp region-configuration** command, you can restore the default MSTP region configurations.

By default, the three MST region parameters take the default values. The MST region name of the switch is the first MAC address, all the VLANs are mapped to CIST, and MSTP revision level takes 0.

You can enter MST region view, using the **stp region-configuration** command. And then you can configure the parameters including region name, revision level, and VLAN mapping table of the region.

Example

```
# Enter MST region view.
[Quidway] stp region-configuration
[Quidway-mst-region]
```

1.1.33 stp tc-protection

Syntax

stp tc-protection enable
stp tc-protection disable

View

System view

Parameter

None
Description

Using the **stp tc-protection enable** command, you can enable the protection function from being attacked by TC-BPDU packets on the switch. Using the **stp tc-protection disable** command, you can disable the protection function.

By default, the protection from TC-BPDU packet attack is enabled.

As a general rule, the switch deletes the corresponding entries in the MAC address table and ARP table upon receiving TC-BPDU packets. When under malicious attacks of TC-BPDU packets, the switch shall receive a great number of TC-BPDU packets in a very short period. Too frequent delete operations shall consume huge switch sources and bring great risk to network stability.

When the protection from TC-BPDU packet attack is enabled, the switch just perform one delete operation in a specified period after receiving TC-BPDU packets, as well as monitoring whether it receives TC-BPDU packets during this period. Even if it detects a TC-BPDU packet is received in a period shorter than the specified interval, the switch shall not run the delete operation till the specified interval is reached. This can avoid frequent delete operations to the MAC address table and ARP table.

Example

```
# Enable TC-BPDU protection on the switch.
[Quidway] stp tc-protection enable
```

### 1.1.34 stp root-protection

**Syntax**

```
stp root-protection
undo stp root-protection
```

**View**

Ethernet port view

**Parameter**

None

**Description**

Using **stp root-protection** command, you can enable on Root protection the switch. Using **undo stp root-protection** command, you can restore the default state of Root protection.

By default, Root protection is disabled.

In case of configuration error or malicious attack, the legal primary root may receive the BPDU with a higher priority and then loose its place, which causes network topology...
change errors. Due to the illegal change, the traffic supposed to travel over the high-speed link may be pulled to the low-speed link and congestion will occur on the network.

MSTP provides Root protection function to protect the root bridge: The port configured with Root protection only plays a role of designated port on every instance. Whenever such port receives a higher-priority BPDU, it will be set to listening state and not forward packets any more (as if the link to the port is disconnected). If the port has not received any higher-priority BPDU for a certain period of time thereafter, it will resume the normal state.

For the related command, see `stp interface root-protection`.

Example

```
# Enable Root protection on the ethernet0/1 port of the switch.
[Quidway-Ethernet0/1] stp root-protection
```

1.1.35 stp timer forward-delay

Syntax

```
stp timer forward-delay centi-senconds
undo stp timer forward-delay
```

View

System view

Parameter

`centi-senconds`: Specifies Forward Delay, ranging from 400 to 3000 and measured in centiseconds. By default, the Forward Delay of the switch is 1500 centiseconds.

Description

Using `stp timer forward-delay` command, you can configure Forward Delay for the switch. Using `undo stp timer forward-delay` command, you can restore the default Forward Delay.

To avoid temporary loop, MSTP defines a medium state, Learning, when the port switches from the Discarding state to Forwarding state. There is also a delay before state switchover to guarantee the synchronous switchover with the remote switch. The Forward Delay configured on the root bridge determines the state transition time. The root bridge will determine the state transition time according to the configured values, while the other switches will apply the forward delay configured on it.

When configuring Hello time, Forward Delay and Max Age, please guarantee the following equations:
2 * (Forward Delay - 1.0 seconds) >= Max Age
Max Age >= 2 * (Hello Time + 1.0 seconds)

Only if the above-mentioned formulas are equal can the MSTP normally operate on the entire network, otherwise, the network may flap frequently. You are recommended to use the stp root primary command to specify the diameter of the switching network, so that MSTP can automatically calculate and give the moderate values for the time parameters.

For the related command, see stp timer hello, stp timer max-age, stp bridge-diameter.

Example

# Set the Forward Delay of the device to 2000 centiseconds.
[Quidway] stp timer forward-delay 2000

1.1.36  stp timer hello

Syntax

stp timer hello centi-seconds
undo stp timer hello

View

System view

Parameter

centi-seconds: Specifies Hello Time value with an integer in the range of 100 to 1000 in units of centiseconds. By default, the Hello Time of the switch is 200 centiseconds.

Description

Using stp timer hello command, you can configure Hello Time of the switch. Using undo stp timer hello command, you can restore the default Hello Time.

The STP defines to transmit configuration BPDU regularly at an interval specified with Hello Time to keep the spanning tree stable. If the switch receives no BPDU packets for a period of time, it will recalculate the spanning tree upon the BPDU timeouts. The root bridge transmits BPDU packets at an interval as you configured, while other switches apply the Hello Time configured on the root bridge.

When configuring Hello time, Forward Delay and Max Age, remember to guarantee the following equations:

2 * (Forward Delay - 1.0 seconds) >= Max Age
Max Age >= 2 * (Hello Time + 1.0 seconds)
Only if the above-mentioned formulas are equal can the MSTP normally operate on the entire network, otherwise, the network may flap frequently. You are recommended to use the stp root primary command to specify the diameter of the switching network, so that MSTP can automatically calculate and give the moderate values for the time parameters.

For the related command, see stp timer forward-delay, stp timer max-age, stp bridge-diameter.

Example

```
# Set Hello Time of the switch 300 centiseconds.
[Quidway] stp timer hello 300
```

1.1.37 stp timer max-age

Syntax

```conf
stp timer max-age centi-secons
```

```
undo stp timer max-age
```

View

System view

Parameter

- **centiseconds**: Specifies the Max Age, ranging from 600 to 4000 and measured with centiseconds. By default, the Max Age of the switch is 2000 centiseconds.

Description

Using **stp timer max-age** command, you can configure the Max Age of the switch. Using **undo stp timer max-age** command, you can restore the default Max Age.

MSTP can detect the link fault and automatically resume the forwarding state of the redundant link. On the CIST, the switch checks if the configuration BPDU received via the port expires according to the Max Age. If the BPDU expires, the STI has to be calculated again.

Max Age takes no effect on MSTIs. If the current switch is CIST root bridge, it will check if the configuration BPDU expires according to the configured Max Age. Otherwise, the switch adopts the Max Age configured on the CIST root bridge.

When you configure Hello time, Forward Delay and Max Age, ensure the following formulas equal:

- \[2 \times (\text{Forward Delay} - 1.0 \text{ seconds}) \geq \text{Max Age}\]
- \[\text{Max Age} \geq 2 \times (\text{Hello Time} + 1.0 \text{ seconds})\]
Only if the above-mentioned formulas are equal can the MSTP normally operate on the entire network, otherwise, the network may flap frequently. You are recommended to use the `stp root primary` command to specify the diameter of the switching network, so that MSTP can automatically calculate and give the moderate values for the time parameters.

For the related command, see `stp timer forward-delay`, `stp timer hello`, `stp bridge-diameter`.

Example

```
# Set Max Age of the device to 1000 centiseconds.
[Quidway] stp timer max-age 1000
```

### 1.1.38 `stp transit-limit`

#### Syntax

```
stp transit-limit packetnum
undo stp transit-limit
```

#### View

Ethernet port view

#### Parameter

`packetnum`: Specifies the amount limit to the transmitted packets, ranging from 1 to 255 (expressed as a counter value without any units). By default, the value is 3.

#### Description

Using `stp transit-limit` command, you can configure an amount limit to the configuration BPDU transmitted via a port during the Hello Time. Using `undo stp transit-limit` command, you can restore the default limit.

The larger the value is, the more packets can be transmitted in a time unit, yet the more switch resources will be occupied. With a moderate value, the amount of the BPDUs transmitted during Hello Time via every port can be limited and MSTP will not occupy too many bandwidth resources when the network topology flaps.

For the related command, see `stp interface transit-limit`.

#### Example

```
# Set a limit of 5 to the packets transmitted via ethernet0/1.
[Quidway-Ethernet0/1] stp transit-limit 5
```
1.1.39 vlan-mapping modulo

Syntax

vlan-mapping modulo modulo

View

MST region view

Parameter

modulo: Specifies the modulus, ranging from 1 to 16.

Description

Using `vlan-mapping modulo` command, you can map a VLAN list to an STI.

By default, all the VLANs are mapped to CIST, namely Instance 0.

MSTP describes the association between VLANs and STIs with the VLAN mapping table. You can use this command to configure this table. Every VLAN can be mapped to an STI as per your configuration.

A VLAN cannot be mapped to different MSTI at the same time. The latter configured association will replace the former one.

The `vlan-mapping modulo modulo` command designates VLAN for every STI fast. It maps the VLAN to an STI whose ID is (VLAN ID-1)\%modulo+1. (Note: (VLAN ID-1) \%modulo performs modulo operation on (VLAN ID-1). Taking the operation modulo 16 as an example, vlan 1 maps to MSTI 1, vlan 2 maps to MSTI2 ...vlan 16 maps to MSTI16, vlan 17 maps to MSTI 1, and so on.)

For the related command, see `region-name`, `revision-level`, `display configuration`, `active configuration`, .

Example

# Map VLAN to STI modulo 16.
[Quidway-mst-region] vlan-mapping modulo 16
Table of Contents

Chapter 1 802.1x Configuration Commands ................................................................. 1-1
  1.1 802.1x Configuration Commands ........................................................................... 1-1
    1.1.1 display dot1x .................................................................................................. 1-1
    1.1.2 dot1x ............................................................................................................. 1-2
    1.1.3 dot1x authentication-method ................................................................. 1-3
    1.1.4 dot1x dhcp-launch ..................................................................................... 1-4
    1.1.5 dot1x dynamic-binding-user enable .......................................................... 1-5
    1.1.6 dot1x guest-vlan ......................................................................................... 1-6
    1.1.7 dot1x max-user ........................................................................................... 1-7
    1.1.8 dot1x port-control ....................................................................................... 1-8
    1.1.9 dot1x port-method ....................................................................................... 1-9
    1.1.10 dot1x quiet-period .................................................................................... 1-10
    1.1.11 dot1x re-authenticate ............................................................................... 1-11
    1.1.12 dot1x retry ................................................................................................ 1-12
    1.1.13 dot1x retry-version-max .......................................................................... 1-13
    1.1.14 dot1x supp-proxy-check .......................................................................... 1-13
    1.1.15 dot1x timer ................................................................................................ 1-15
    1.1.16 dot1x version-check ................................................................................ 1-16
    1.1.17 reset dot1x statistics ................................................................................. 1-17

Chapter 2 AAA & RADIUS Protocol Configuration Commands ....................................... 2-1
  2.1 AAA Configuration Commands ............................................................................ 2-1
    2.1.1 access-limit ............................................................................................... 2-1
    2.1.2 attribute ..................................................................................................... 2-2
    2.1.3 cut connection ........................................................................................... 2-3
    2.1.4 display connection .................................................................................... 2-4
    2.1.5 display domain .......................................................................................... 2-5
    2.1.6 display local-user ....................................................................................... 2-6
    2.1.7 domain ....................................................................................................... 2-8
    2.1.8 idle-cut ....................................................................................................... 2-9
    2.1.9 local-user .................................................................................................... 2-10
    2.1.10 local-user password-display-mode ........................................................... 2-11
    2.1.11 messenger ............................................................................................... 2-11
    2.1.12 name ........................................................................................................ 2-12
    2.1.13 password ................................................................................................ 2-13
    2.1.14 radius-scheme ......................................................................................... 2-14
    2.1.15 self-service-url ........................................................................................ 2-14
    2.1.16 service-type ............................................................................................. 2-15
# Table of Contents

**2.1.17 state** ..................................................................................................................... 2-16
**2.1.18 vlan-assignment-mode** ........................................................................................ 2-17

## 2.2 RADIUS Protocol Configuration Commands ................................................................... 2-18

2.2.1 accounting-on enable ............................................................................................ 2-18
2.2.2 accounting optional ............................................................................................... 2-20
2.2.3 data-flow-format .................................................................................................... 2-20
2.2.4 display local-server statistics ................................................................................. 2-21
2.2.5 display radius ........................................................................................................ 2-22
2.2.6 display radius statistics ......................................................................................... 2-23
2.2.7 display stop-accounting-buffer .............................................................................. 2-24
2.2.8 key ......................................................................................................................... 2-25
2.2.9 local-server ............................................................................................................ 2-26
2.2.10 nas-ip ................................................................................................................... 2-27
2.2.11 primary accounting .............................................................................................. 2-28
2.2.12 primary authentication ......................................................................................... 2-29
2.2.13 radius nas-ip ........................................................................................................ 2-30
2.2.14 radius scheme ..................................................................................................... 2-31
2.2.15 reset radius statistics ........................................................................................... 2-32
2.2.16 reset stop-accounting-buffer .............................................................................. 2-32
2.2.17 retry ..................................................................................................................... 2-33
2.2.18 retry realtime-accounting..................................................................................... 2-34
2.2.19 retry stop-accounting........................................................................................... 2-35
2.2.20 secondary accounting ......................................................................................... 2-36
2.2.21 secondary authentication .................................................................................... 2-36
2.2.22 server-type .......................................................................................................... 2-37
2.2.23 state ..................................................................................................................... 2-38
2.2.24 stop-accounting-buffer enable ............................................................................. 2-39
2.2.25 timer .................................................................................................................... 2-40
2.2.26 timer quiet ............................................................................................................ 2-41
2.2.27 timer realtime-accounting .................................................................................... 2-41
2.2.28 user-name-format ................................................................................................ 2-42

## 3.1 HABP Commands ........................................................................................................... 3-1

3.1.1 display debugging habp .......................................................................................... 3-1
3.1.2 display habp .......................................................................................................... 3-1
3.1.3 display habp table .................................................................................................. 3-2
3.1.4 display habp traffic ............................................................................................... 3-3
3.1.5 habp enable .......................................................................................................... 3-3
3.1.6 habp server vlan ................................................................................................... 3-4
3.1.7 habp timer ............................................................................................................. 3-4
Chapter 1  802.1x Configuration Commands

1.1  802.1x Configuration Commands

1.1.1  display dot1x

Syntax

    display dot1x [ sessions | statistics ] [ interface interface-list ]

View

Any view

Parameter

sessions: Configures to display the session connection information of 802.1x.
statistics: Configures to display the relevant statistics information of 802.1x.
interface: Configures to display the 802.1x information on the specified 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, read the Parameter of the Port Command Manual section.

Description

Using display dot1x command, you can view the relevant information of 802.1x, including configuration information, running state (session connection information) and relevant statistics information.

If no port is specified when executing this command, the system will display all 802.1x related information. The output information of this command can help the user to verify the current 802.1x configurations so as to troubleshoot 802.1x.

For the related commands, see 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.
    <Quidway> display dot1x
Equipment 802.1X protocol is enabled
CHAP authentication is enabled
DHCP-launch is disabled
Dynamic-binding-user is disabled
Proxy trap checker is disabled
Proxy logoff checker is disabled

Configure: Transmit Period 30 s, Commit Period 15 s
ReAuth Period 3600 s
Quiet Period 60 s, Value of Quiet Period Timer is disabled
Supp Timeout 30 s, Value of Server Timeout 000100 s
The maximal retransmitting times 3
Handshake period 15 s

Total maximum on-line user number is 1024
Total current on-line user number is 0

Ethernet0/1 is link-up
802.1X protocol is disabled
Proxy trap checker is disabled
Proxy logoff checker is disabled
Version-Check is disabled
The port is a(n) authenticator
Authenticate Mode is auto
Port Control Type is Mac-based
ReAuthenticate is disabled
Max on-line user number is 256
... (Omitted)

1.1.2 dot1x

Syntax

```
dot1x [ interface interface-list ]
undo dot1x [ interface interface-list ]
```

View

System 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` |...
The command syntax is:

```
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

Using **dot1x** command, you can enable 802.1x on the specified port or globally (i.e., on the current device). Using **undo dot1x** command, you can 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 input 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.

For the related commands, see **display dot1x**.

### Example

```
# Enable 802.1x on Ethernet 0/1.
[Quidway] dot1x interface Ethernet 0/1

# Enable the 802.1x globally.
[Quidway] dot1x
```

### 1.1.3 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**

Using **dot1x authentication-method** command, you can configure the authentication method for 802.1x user. Using **undo dot1x authentication-method** command, you can restore the default authentication method of 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 password in the form of simple text.

Challenge Handshake Authentication Protocol (CHAP) is a kind of authentication protocol with three handshakes. It only transmits username but not password. CHAP is more secure and reliable.

In the process of EAP authentication, switch directly sends authentication information of 802.1x user to RADIUS server in the form of EAP packet. It is not necessary to transfer the EAP packet to standard RADIUS packet first and then send it to RADIUS server. By now, for EAP authentication, PEAP, EAP-TLS and EAP-MD5 methods are available.

If you want to enable PEAP, EAP-TLS or EAP-MD5 authentication method on an Ethernet switch, you only need to use the command **dot1x authentication-method eap** to enable EAP authentication.

Please note: To realize PAP, CHAP or EAP authentication, RADIUS server should support PAP, CHAP or EAP authentication respectively.

For the related command, see **display dot1x**.

**Example**

```bash
# Configure 802.1x user to use PAP authentication.
[Quidway] dot1x authentication-method pap
```

### 1.1.4 dot1x dhcp-launch

**Syntax**

```
dot1x dhcp-launch
undo dot1x dhcp-launch
```

**View**

System view

**Parameter**

None
Description

Using **dot1x dhcp-launch** command, you can set 802.1x to disable the switch to trigger the user ID authentication over the users who configure static IP addresses in DHCP environment. Using **undo dot1x dhcp-launch** command, you can set 802.1x to enable the switch to trigger the authentication over them.

By default, the switch can trigger the user ID authentication over the users who configure static IP addresses in DHCP environment.

For the related command, see **dot1x**.

Example

```bash
# Disable the switch to trigger the authentication over the users who configure static IP addresses in DHCP environment.
[Quidway] dot1x dhcp-launch
```

### 1.1.5 **dot1x dynamic-binding-user enable**

**Syntax**

```
dot1x dynamic-binding-user enable  
undo dot1x dynamic-binding-user enable
```

**View**

System view

**Parameter**

None

**Description**

Use the **dot1x dynamic-binding-user enable** command to enable 802.1x dynamic user binding.

Use the **undo dot1x dynamic-binding-user enable** command to disable 802.1x dynamic user binding.

802.1x dynamic user binding is disabled by default.

802.1x dynamic user binding enables a switch to dynamically bind the IP address, the MAC address, the accessing port, and the VLAN to which the accessing port belongs after an 802.1x user passes the authentication. And the switch then only permits the packets that match all these four items. If the switch finds that the four items carried in the packets sent by the user are not consistent with the bound ones, it will force the user to go offline.

Note that:
1) If the users obtain their IP addresses dynamically, you must couple dynamic user binding with DHCP Snooping in the following way:
   - Enable DHCP Snooping globally on the switch.
   - Configure the switch port connecting to the DHCP server to be a DHCP Snooping trusted port.

2) If the users use static IP addresses, they must use 802.1x clients developed by Huawei Technologies and select the Upload user IP address option in the [802.1x Network Settings] dialog box when creating a new connection.

Related command: dot1x.

Example

```
# Enable 802.1x dynamic user binding.
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] dot1x dynamic-binding-user enable
```

1.1.6 dot1x guest-vlan

Syntax

```
dot1x guest-vlan vlan-id [ interface interface-list ]
undo dot1x guest-vlan vlan-id [ interface interface-list ]
```

View

System view/Ethernet port view

Parameter

- `vlan-id`: ID of Guest VLAN, ranging from 1 to 4094.
- `interface_list`: Enable the Guest VLAN interface list. `interface_list = \{ interface_type interface_num | interface_name \} \[ to \{ interface_type interface_num | interface_name \} \] \&<1-10>`. Note that after the key work `to`, the port number must be equal to or greater than the port number before `to`. \&<1-10> means the parameter before it can be input repeatedly for 10 times.

Description

Using the `dot1x guest-vlan` command, you can enable the Guest VLAN function on specified port. Using the `undo dot1x guest-vlan` command, you can disable this function.

When you execute this command in system view, if you do not input the `interface-list` parameter, it means that to enable Guest VLAN on all ports; if you specify this parameter, it means that to enable Guest VLAN on the specified port.
When you execute this command in Ethernet port view, you can only enable Guest VLAN on the current port, and the \textit{interface-list} parameter cannot be input.

Note the following:

- Guest VLAN is only supported in the port-based authentication mode.
- A switch only can be configured with one Guest VLAN.
- Users who skip the authentication, fail in the authentication or get offline belong to the Guest VLAN.
- If \texttt{dot1x dhcp-launch} is configured on the switch, the Guest VLAN function cannot be implemented because the switch does not send active authentication packet in this mode.

Example

```bash
# Set the authentication mode to port-based.
[Quidway] dot1x port-method portbased

# Enable Guest VLAN on all ports.
[Quidway] dot1x guest-vlan 1
```

1.1.7 \texttt{dot1x max-user}

Syntax

\begin{verbatim}
dot1x max-user user-number [ interface interface-list ]
undo dot1x max-user [ interface interface-list ]
\end{verbatim}

View

System view/Ethernet port view

Parameter

\textit{user-number}: Specifies the limit to the amount of supplicants on the port, ranging from 1 to 256.

By default, the maximum user number is 256.

\textit{interface interface-list}: Ethernet interface list including several Ethernet interfaces, expressed in the format \texttt{interface-list = \{ interface-num [ to interface-num ] \} & < 1-10 >}.

\texttt{interface-num} specifies a single Ethernet interface in the format \texttt{interface-num = \{ interface-type interface-num | interface-name \}}, where \texttt{interface-type} specifies the interface type, \texttt{interface-num} specifies the interface number and \texttt{interface-name} specifies the interface name. For the respective meanings and value ranges, read the Parameter of the Port Command Manual section.
Description

Using `dot1x max-user` command, you can configure a limit to the amount of supplicants on the specified interface of 802.1x. Using `undo dot1x max-user` command, you can 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 has effect on the interface specified by the parameter `interface-list` when executed in system view. It has 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 effect only on the current interface.

For the related commands, see `display dot1x`.

Example

```
# Configure the interface Ethernet 0/1 to hold no more than 32 users.
[Quidway] dot1x max-user 32 interface Ethernet 0/1
```

1.1.8 dot1x port-control

Syntax

```
dot1x port-control { auto | authorized-force | unauthorized-force } [ interface interface-list ]
undo dot1x port-control [ interface interface-list ]
```

View

System view/Ethernet port view

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 \( \text{interface-num} = \{ \text{interface-type} \ \text{interface-num} | \text{interface-name} \} \), 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, read the Parameter of the Port Command Manual section.

**Description**

Using **dot1x port-control** command, you can configure the mode for 802.1x to perform access control on the specified interface. Using **undo dot1x port-control** command, you can 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 effect on the interface specified by the parameter **interface-list** when executed in system view. It has 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 effect only on the current interface.

For the related commands, see **display dot1x**.

**Example**

```
# Configure the interface Ethernet 0/1 to be in unauthorized-force state.
[Quidway] dot1x port-control unauthorized-force interface Ethernet 0/1
```

**1.1.9 dot1x port-method**

**Syntax**

```
dot1x port-method { macbased | portbased } [ interface interface-list ]
undo dot1x port-method [ interface interface-list ]
```

**View**

System view/Ethernet Port view

**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 \( \text{interface-list} = \{ \text{interface-num} | \text{to interface-num} \} \) & & 1-10 > . interface-num specifies a single Ethernet interface in the format \( \text{interface-num} = \)
{ 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, read the Parameter of the Port Command Manual section.

**Description**

Using `dot1x port-method` command, you can configure the base for 802.1x to perform access control on the specified interface. Using `undo dot1x port-method` command, you can 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 adopted, the user access this interface must be authenticated independently, and if one successful authentication user is to finish network service, the other accessed users can still use network service. When `portbased` is adopted, if only the first access user by this interface can be authenticated successfully, the other access users followed can be considered authenticated successfully automatically, but if the first one finish the network service, the other accessed users' network service will be rejected.

This command has effect on the interface specified by the parameter **interface-list** when executed in system view. It has 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 effect only on the current interface.

For the related commands, see `display dot1x`.

**Example**

```
# Authenticate the supplicant based on the interface number on Ethernet 0/1.
[Quidway] dot1x port-method portbased interface Ethernet 0/1
```

### 1.1.10 dot1x quiet-period

**Command**

```
dot1x quiet-period
undo dot1x quiet-period
```

**View**

System view

**Parameter**

None
Description

Using **dot1x quiet-period** command, you can enable the quiet-period timer. Using **undo dot1x quiet-period** command, you can disable this 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.

By default, **quiet-period** timer is disabled.

For the related commands, see **display dot1x**, **dot1x timer**.

Example

```bash
# Enable quiet-period timer.
[Quidway] dot1x quiet-period
```

### 1.1.11 dot1x re-authenticate

**Syntax**

- **dot1x re-authenticate [ interface interface-list ]**
- **undo dot1x re-authenticate [ interface interface-list ]**

**View**

System view/Ethernet port view

**Parameter**

- **interface interface-list**: Ethernet interface list, represents multiple Ethernet interfaces, in the format of **interface-list = { interface-num [ to interface-num ] } & < 1-10 >**. **interface-num** is a single Ethernet port, in the format of **interface-num = { interface-type interface-num | interface-name }**.

**Description**

Using the **dot1x re-authenticate** command, you can enable 802.1x re-authentication on a specific port or all the authenticator ports on a device.

Using the **undo dot1x re-authenticate** command, you can disable 802.1x re-authentication on a specific port or all the authenticator ports on a device.

By default, 802.1x re-authentication is disabled on all ports.

In system view, if the **interface-list** parameter is not specified, it means that to enable the 802.1x re-authentication feature on all interfaces; if the **interface-list** parameter is specified, it means that to enable the feature on the specified interfaces. In Ethernet port view, the **interface-list** parameter cannot be specified, and you can use command only to enable the feature on the current interface.
Before configuring 802.1x re-authentication feature on a port, you must enable the feature both globally and on this port.

Example

```plaintext
# Enable 802.1x reauthentication on port Ethernet 0/1.
[Quidway-Ethernet0/1] dot1x re-authenticate
Re-authentication is enabled on port Ethernet 0/1
```

### 1.1.12 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 for 3 times.

**Description**

Using `dot1x retry` command, you can configure the maximum times an Ethernet switch can retransmit the authentication request frame to the supplicant. Using `undo dot1x retry` command, you can restore the default maximum retransmission time.

After the switch has transmitted 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 for specifying 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 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 effect on all the port after configuration.

For the related commands, see `display dot1x`.

**Example**

```plaintext
# Configure the current device to transmit authentication request frame to the user for no more than 9 times.
[Quidway] dot1x retry 9
```
1.1.13  dot1x retry-version-max

Syntax

    dot1x retry-version-max max-retry-version-value
    undo dot1x retry-version-max

View

    System view

Parameter

    max-retry-version-value: The maximum retry times for a device to send the version request frame to an access user. The value ranges from 1 to 10, and defaults to 3.

Description

Using the `dot1x retry-version-max` command, you can set the maximum retry times for an Ethernet switch to send version request frame to an access user. Using the `undo dot1x retry-version-max` command, you can return the value to the defaults.

After sending client version request frame for the first time, if the switch receives no response from the client response within a certain period of time (set by the version authentication timeout timer), it resends version request again. When the switch receives no response for the configured maximum times, it no longer authenticates the version of the client, and perform the following authentications. If configured, this command functions on all ports that enabled version authentication function.

See `display dot1x` and `dot1x timer` for related configuration.

Example

    # Configure the switch to send version request frame to an access user 6 times at the most.
    [Quidway] dot1x retry-version-max 6

1.1.14  dot1x supp-proxy-check

Syntax

    dot1x supp-proxy-check { logoff | trap } [ interface interface-list ]
    undo dot1x supp-proxy-check { logoff | trap } [ interface interface-list ]

View

    System view/Ethernet Port view
Parameter

logoff: Cuts network connection to a user upon detecting the use of proxy.
trap: Sends 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, read the Parameter of the Port Command Manual section.

Description

Using dot1x supp-proxy-check command, you can configure the control method for 802.1x access users via proxy logon the specified interface. Using undo dot1x supp-proxy-check command, you can cancel the control method set for the 802.1x access users via proxy.

Note that when performing this function, the user logging on via proxy need to run Huawei 802.1x client program, (Huawei 802.1x client program version V1.29 or above is needed).

This command is used to set 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 has 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 effects on the port.

For the related command, see display dot1x.

Example

# Configure the switch cut network connection to a user upon detecting the use of proxy on Ethernet 0/1 ~ Ethernet 0/8.
[Quidway] dot1x supp-proxy-check logoff
[Quidway] dot1x supp-proxy-check logoff interface Ethernet 0/1 to Ethernet 0/8

# Configure the switch to send trap message upon detecting the use of proxy on Ethernet 0/9.
[Quidway] dot1x supp-proxy-check trap
[Quidway] dot1x supp-proxy-check trap interface Ethernet 0/9

or

[Quidway] dot1x supp-proxy-check trap
[Quidway] interface Ethernet 0/9
[Quidway-Ethernet0/9] dot1x supp-proxy-check trap
1.1.15 dot1x timer

Syntax

```
dot1x timer { handshake-period handshake-period-value | quiet-period quiet-period-value | reauth-period reauth-period-value | server-timeout server-timeout-value | supp-timeout supp-timeout-value | tx-period tx-period-value | ver-period ver-period-value }
```

```
undo dot1x timer { handshake-period | quiet-period | reauth-period | server-timeout | supp-timeout | tx-period | ver-period }
```

View

System view

Parameter

- **handshake-period**: This timer begins after the user has passed the authentication. After setting handshake-period, system will send the handshake packet by the period. Suppose the dot1x retry time is configured as N, the system will consider the user having logged off and set the user as logoff state if system doesn’t receive the response from user for consecutive N 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 in units of second 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 in units of second and defaults to 30.
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, the tx-period 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 in units of second and defaults to 30.

reauth-period: Re-authentication timeout timer. During the time limit set by this timer, the supplicant device launches 802.1x re-authentication.

*reauth-period-value*: Period set by the re-authentication timeout timer, ranging from 1 to 86400, in seconds. By default, the value is 3600.

ver-period: Client version request timeout timer. If the supplicant device failed to send the version response packet within the time set by this timer, then the authenticator device will resend the version request packet.

*ver-period-value*: Period set by the version request timeout timer, ranging from 1 to 30, in seconds. By default, the value is 1.

**Description**

Using `dot1x timer` command, you can configure the 802.1x timers. Using `undo dot1x timer` command, you can restore the default values.

When it is run, 802.1x enables many timers to control the rational and orderly interacting of the Supplicant, the Authenticator and the Authenticator Server. This command can set some of the timers (while other timers cannot be set) to adapt the interaction process. It could be necessary for some special and hard network environment. Generally, the user should keep the default values of the timers.

For the related commands, see `display dot1x`.

**Example**

```
# Set the Authentication Server timeout timer is 150s.
[Quidway] dot1x timer server-timeout 150
```

**1.1.16 dot1x version-check**

**Syntax**

```
dot1x version-check [ interface interface-list ]
undo dot1x version-check [ interface interface-list ]
```

**View**

System view/Ethernet port view
Parameter

`interface interface-list` Ethernet interface list, represents multiple Ethernet interfaces, in the format of `interface-list = { interface-num [ to interface-num ] } & < 1-10 >. interface-num` is a single Ethernet port, in the format of `interface-num = { interface-type interface-num | interface-name }`.

Description

Using the `dot1x version-check` command, you can enable the 802.1x client version authentication feature on a specific port. Using the `undo dot1x version-check` command, you can disable the feature on a specific port.

By default, 802.1x client version authentication feature is disabled on all ports.

In system view, if the `interface-list` parameter is not specified, it means that to enable the 802.1x client version authentication feature on all interfaces; if the `interface-list` parameter is specified, it means that to enable the feature on the specified interfaces. In Ethernet port view, the `interface-list` parameter cannot be specified, and you can use command only to enable the feature on the current interface.

Example

# Configure the port Ethernet 0/1 to detect the version of the 802.1x client when it receives an authentication packet.

```
[Quidway-Ethernet0/1] dot1x version-check
```

1.1.17 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 of `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

Using `reset dot1x statistics` command, you can 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 is 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.

For the related commands, see `display dot1x`.

**Example**

```
# Clear the 802.1x statistics on Ethernet 0/1.
<Quidway> reset dot1x statistics interface Ethernet 0/1
```
Chapter 2  AAA & RADIUS Protocol Configuration

Commands

2.1  AAA Configuration Commands

2.1.1  access-limit

Syntax

    access-limit { disable | enable max-user-number }

    undo access-limit

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 1024.

Description

Using access-limit command, you can configure a limit to the amount of supplicants in the current ISP domain. Using undo access-limit command, you can restore the limit to the default setting.

By default, there is no limit to the amount of supplicants in the current ISP domain.

The access-limit command limits the amount of supplicants contained in the current ISP domain. The supplicants may contend for the network resources. So setting a suitable limit to the amount will guarantee the reliable performance for the existing supplicants.

Example

    # Set a limit of 500 supplicants for the ISP domain named huawei163.net.
    [Quidway-isp-huawei163.net] access-limit enable 500
2.1.2 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 H-H-H.
- **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 locate.) 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 access users who access the device by 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 belong. 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 with 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 can be used to replace it.

Description

Using **attribute** command, you can configure some attributes for specified local user. Using **undo attribute** command, you can 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.
For the related command, see `display local-user`.

Example

```
# Configure the IP address 10.110.50.1 to the user huawei1.
[Quidway-luser-huawei1] attribute ip 10.110.50.1
```

2.1.3 cut connection

Syntax

```
cut connection { all | access-type dot1x | 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**: Configures to cut a category of connections according to logon type. dot1x means the 802.1x 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.
- **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 so on. 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**

Using **cut connection** command, you can disconnect a user or a category of users by force.

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

**Example**

# Cut all the connections in the ISP domain, huawei163.net.

[Quidway] cut connection domain huawei163.net

### 2.1.4 display connection

**Syntax**

```
display connection [ access-type dot1x | 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**

Any view

**Parameter**

- **access-type**: Configures to display the supplicants according to their logon type. **dot1x** means the 802.1x 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 **ip-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**.
**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 80 characters, excluding “”, “.”, “””, “?”,”<”, “>”, and so on. 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**

Using **display connection** command, you can 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.

For the related command, see **cut connection**.

**Example**

```
# Display the relevant information of all the users.
<Quidway> display connection
Total 0 connections matched, 0 listed.
```

### 2.1.5 display domain

**Syntax**

```
display domain [ isp-name ]
```

**View**

Any view

**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**

Using **display domain** command, you can 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 will be displayed exactly the same, concerning the content and format, 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.
For the related commands, see access-limit, domain, radius scheme, state, display domain.

Example

# Display the summary information of all ISP domains of the system.
<Quidway> display domain
0  Domain = system
   State = Active    Access-limit = Disable
   Vlan-assignment-mode = Integer
   Domain User Template:
      Idle-cut = Disable
      Self-service = Disable
      Messenger Time = Disable

   Default Domain Name: system
   Total 1 domain(s): 1 listed.

2.1.6 display local-user

Syntax

display local-user [ domain isp-name | idle-cut { enable | disable } ] service-type
   { telnet | ftp | ssh | lan-access } state { active | block } user-name user-name | vlan vlanid ]

View

Any view

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 will 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. 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, excluding "/", ":", "*", "?", "<", ">", and so on. The @ character can only be used once in one username. The pure username (the part before @, namely the user ID) cannot exceed 55 characters.

vlan vlanid: Configures to display the users belonged to specified VLAN. vlanid is the integer, ranging from 1 to 4094.

Description

Using display local-user command, you can 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.

For the related command, see local-user.

Example

# Display the relevant information of all the local users.
<Quidway> display local-user
The contents of local user user1:
State: Active ServiceType Mask: T
Idle-cut: Disable
Access-limit: Disable Current AccessNum: 0
Bind location: Disable
Vlan ID: Disable
IP address: Disable
MAC address: Disable
User Privilege: 1

Total 1 local user(s) Matched, 1 listed.

Table 2-1 Output description of the display local-user command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>The state of the user</td>
</tr>
<tr>
<td>Idle-Cut</td>
<td>The state of the idle-cut switch</td>
</tr>
<tr>
<td>Access-Limit</td>
<td>The limit to the number of access users.</td>
</tr>
<tr>
<td>Bind location</td>
<td>Indicates whether the port is bound with or not</td>
</tr>
</tbody>
</table>
### 2.1.7 domain

**Syntax**

```plaintext
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 so on.
- `default enable isp-name`: Enables the default ISP domain specified by `isp-name`.
- `default disable`: Restores the default ISP domain to `system`.

**Description**

Using `domain` command, you can configure an ISP domain or enter the view of an existing ISP domain. Using `undo domain` command, you can 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@huawei163.net` as an example, the `isp-name` (i.e. `huawei163.net`) following the `@` is the ISP domain name. When Quidway 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 to configure 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.

For the related commands, see access-limit, radius scheme, state, display domain.

Example

# Create a new ISP domain, huawei163.net, and enters its view.
[Quidway] domain huawei163.net
New Domain added.
[Quidway-isp-huawei163.net]

2.1.8 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 idle-cut 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

Using idle-cut command, you can 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.

For the related command, see domain

Example

# Enable the user in the current ISP domain, huawei163.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.

[Quidway-isp-huawei163.net] idle-cut enable 50 500

2.1.9 local-user

Syntax

local-user user-name
undo local-user { user-name | all | service-type { telnet | ftp | lan-access | ssh } }

View

System view

Parameter

user-name: Specifies a local username with a character string not exceeding 80 characters, excluding “/”, “:”, “*”, “?” “<”, “>” and so on. 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 is case-insensitive, so that UserA is the same as UserA.

service-type: Specifies the service type. telnet means that: the specified user type is telnet. ftp means that: the specified user type is ftp. lan-access means that the specified user type is lan-access which mainly refers to Ethernet accessing users, 802.1x supplicants for example. ssh means the specified user type is SSH.

all: All the users.

Description

Using local-user command, you can configure a local user and enter the local user view. Using undo local-user command, you can cancel a specified local user.

By default, no local user.

For the related commands, see display local-user , service-type.
Example

# Add a local user named huawei1.
[Quidway] local-user huawei1
[Quidway-luser-huawei1]

2.1.10 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

Using local-user password-display-mode command, you can configure the password display mode of all the accessing users. Using undo local-user password-display-mode command, you can cancel the password display mode that has been set for all the accessing users.
If cipher-force has been adopted, the user efforts of specifying to display passwords in simple text will render useless.
The password display mode of all the accessing users defaults to auto.
For the related commands, see display local-user , password.

Example

# Force all the accessing users to display passwords in cipher text.
[Quidway] local-user password-display-mode cipher-force

2.1.11 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. It 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

# 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.

[Quidway-isp-system] messenger time enable 30 5

2.1.12 name

Syntax

name string

undo name
View

VLAN view

Parameter

string: Name of the delivered VLAN.

Description

Using name command, you can configure name of the delivered VLAN.
For the related commands, see vlan-assignment-mode.

Example

# Configure name of the delivered VLAN

[Quidway-vlan100] name test

2.1.13  password

Syntax

password { simple | cipher } password

undo password

View

Local user view

Parameter

simple: Specifies to display passwords in simple text.
cipher: Specifies to display passwords in cipher 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, for example, huawei918. The password must be an encrypted string of 24 characters in length, for example, _(_TT8F\Y\5SQ=^Q`MAF4<1!!.

Description

Using password command, you can configure a password display mode for local users. Using undo password command, you can cancel the specified password display mode.

If local-user password-display-mode cipher-force has been adopted, the user efforts of using the password command to set the password display mode to simple text (simple) will render useless.

For the related command, see display local-user.
Example

# Set the user huawei1 to display the password in simple text, given the password is 20030422.
[Quidway-luser-huawei1] password simple 20030422

2.1.14 radius-scheme

Syntax

radius-scheme radius-scheme-name
undo radius-scheme

View

ISP domain view

Parameter

radius-scheme-name: Specifies a RADIUS server group, with a character string not exceeding 32 characters.

Description

Using radius-scheme command, you can configure the RADIUS server group used by the current ISP domain. Using undo radius-scheme command, you can restore the RADIUS server group used by the current ISP domain to the default RADIUS server group.

After an ISP domain is created, it uses the default RADIUS server group (named as system. For configuration of relevant parameters, read the RADIUS Configuration section of this chapter ) of the system.

This command is used to specify the RADIUS server group for the current ISP domain. The specified RADIUS server group shall have been created.

For the related commands, see radius scheme, display radius.

Example

# The following example designates the current ISP domain, huawei163.net, to use the RADIUS server, huawei.
[Quidway-isp-huawei163.net] radius-scheme Huawei

2.1.15 self-service-url

Syntax

self-service-url enable url-string
self-service-url disable

Huawei Technologies Proprietary
Command Manual - Security
Quidway S3000-EI Series Ethernet Switches
Chapter 2  AAA & RADIUS Protocol Configuration
Commands

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 default ISP domain "system", 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.
[Quidway] domain system
[Quidway-isp-system] self-service-url enable
http://10.153.89.94/selfservice/modPasswd1x.jsp|userName

2.1.16 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 }* [ level ] }

Huawei Technologies Proprietary
View

Local user view

Parameter

telnet: Specifies user type as Telnet.
ssh: Specifies user type as SSH.
level level: Specifies the level of Telnet or SSH users. The argument level is an integer in the range of 0 to 3 and defaults to 1.
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.

Description

Using service-type command, you can configure a service type for a particular user. Using undo service-type command, you can cancel the specified service type for the user.

Example

# Set to provide the lan-access service for the user huawei1.
[Quidway-luser-huawei1] service-type lan-access

2.1.17 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**

Using `state` command, you can 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.

For the related command, see `domain`.

**Example**

```
# Set the current ISP domain huawei163.net to be in the block state. The supplicants in this domain cannot request for the network service.
[Quidway-isp-huawei163.net] state block

# Set the user huawei1 to be in the block state.
[Quidway-luser-huawei1] state block
```

**2.1.18 vlan-assignment-mode**

**Syntax**

```
vlan-assignment-mode { integer | string }
```

**View**

ISP domain view

**Parameter**

- **integer**: Specify the dynamic VLAN delivery mode as integer.
- **string**: Specify the dynamic VLAN delivery mode as string.

**Description**

Using `vlan-assignment-mode` command, you can specify the dynamic VLAN delivery mode.

Currently the switch supports RADIUS server delivers the integer type and string type VLAN ID.

- Integer VLAN ID: The switch adds the port into the VLAN based on the integer ID delivered from the server. If the VLAN does not exist, it first creates a VLAN and then adds the port into the new VLAN.
- String ID: The switch compares the string ID delivered from the server with the VLAN names existing on the switch. If a matching entry is found, the switch adds the port into the corresponding VLAN. Otherwise, the delivery fails and the user cannot pass the authentication.

By default, the integer mode is selected, that is, the switch supports the RADIUS server delivering the integer VLAN ID.

---

**Note:**

For the string delivery mode, the switch follows this rule in handling strings: If the RADIUS server delivers VLANs with full number string IDs (1024 for example) and their converted integer form is within the VLAN range, the switch just handles them as integer IDs and add the authentication port to the VLAN with the corresponding integer ID. In this example, the port is added into VLAN 1024.

---

For the related commands, see `name`.

**Example**

```
# Specify the dynamic VLAN delivery mode as integer.
[Quidway-isp-ias] vlan-assignment-mode integer
```

### 2.2 RADIUS Protocol Configuration Commands

#### 2.2.1 accounting-on enable

**Syntax**

```
accounting-on enable [ send times ] [ interval interval ]
undo accounting-on { enable | send | interval }
```

**View**

RADIUS Scheme view

**Parameter**

- `times`: Maximum number for sending Accounting-On packets. It ranges from 1 to 256 and defaults to 15.
- `interval`: Time interval for sending Accounting-On packets. It ranges from 1 to 30 in seconds and defaults to 3.
Description

Using the `accounting-on enable` command, you can enable user re-authentication at reboot. Using the `undo accounting-on enable` command, you can disable this function.

Using the `undo accounting-on send` command, you can restore the default number for sending Accounting-On packets.

Using the `undo accounting-on interval` command, you can restore the default time interval for sending Accounting-On packets.

By default, user re-authentication at reboot is disabled.

Exclusive users are those with its concurrent online number set to 1 on the CAMS. In the AAA solution implemented jointly by the switch and CAMS, if the switch reboots after a user passes the authentication/authorization begins being accounted, the switch prompts that the user has been online when the user logs into the switch before CAMS makes online detection. Therefore, the user cannot access network resources normally. The user can access the network only after the network administrator deletes manually the online information of the user.

To solve this problem, user re-authentication at reboot is designed. After this function is enabled, each time the switch reboots,

- The switch generates an Accounting-On message, which mainly includes NAS-ID, NAS-IP (source IP) and session ID;
- The switch sends to CAMS an Accounting-On message;
- Upon receiving the CAMS Accounting-On message, CAMS finds and deletes the existing online information of the user based on the NAS-ID, NAS-IP (source IP) and session ID in the Accounting-On message.

Note:
The main attributes of the Accounting-On message — NAS-ID, NAS-IP and session ID are often generated automatically by the switch. However, you can configure the NAS-IP using the `nas-ip` command. Make sure you set a correct and valid NAS-IP address. Otherwise, the switch automatically selects the IP address of the virtual VLAN interface as NAS-IP.

Example

```bash
# Enable user reauthentication at reboot.
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] radius scheme CAMS
```
2.2.2 accounting optional

Syntax

accounting optional
undo accounting optional

View

RADIUS scheme view

Parameter

None

Description

Using the accounting optional command, you can enable the selection of RADIUS accounting option. Using the undo accounting optional command, you can disable the selection of RADIUS accounting option.

By default, selection of 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.

Example

# Enable the selection of RADIUS accounting of the RADIUS scheme named as CAMS.
[Quidway-radius-cams] accounting-on enable

2.2.3 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

Using **data-flow-format** command, you can configure the unit of data flow that send to RADIUS Server. Using **undo data-flow-format** command, you can restore the unit to the default setting.

By default, the data unit is byte and the data packet unit is one-packet.

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

Example

# Set the unit of data flow that send to RADIUS Server Huawei is kilo-byte and the data packet unit is kilo-packet.
[Quidway-radius-huawei] data-flow-format data kilo-byte packet kilo-packet

2.2.4 display local-server statistics

Syntax

display local-server statistics

View

Any view

Parameter

None

Description

Using **display local-server statistics** command, you can view the statistics of local RADIUS authentication server.
For the related command, see `local-server`.

**Example**

# Display the statistics of local RADIUS authentication server.

```bash
<Quidway> 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
```

## 2.2.5 display radius

**Syntax**

```bash
display radius [ radius-scheme-name ]
```

**View**

Any view

**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**

Using `display radius` command, you can 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.

For the related command, see `radius scheme`.

**Example**

# Display the configuration information of all the RADIUS schemes.

```bash
<Quidway> display radius
------------------------------------------------------------------
Index=0    Type=huawei
SchemeName  =system          Port=1645   State=block
Primary Auth IP  =127.0.0.1  Port=1646   State=block
Primary Acct IP  =127.0.0.1   Port=1812   State=block
Second Auth IP  =0.0.0.0    Port=1813   State=block
Second Acct IP  =0.0.0.0    Port=1813   State=block
Auth Server Encryption Key= huawei
```
2.2.6 display radius statistics

Syntax

```
display radius statistics
```

View

Any view

Parameter

None

Description

Using the `display radius statistics` command, you can view the statistics information of RADIUS packets. This command outputs the statistics information about the RADIUS packets. The displayed packet information can help with RADIUS diagnosis and troubleshooting.

For the related command, see `radius scheme`.

Example

```
# Display the statistics information of RADIUS packets.
<Quidway> display radius statistics
state statistic(total=1288):
    DEAD=1288    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:
```

Huawei Technologies Proprietary
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
... (Omitted)

2.2.7  display stop-accounting-buffer

Syntax

display stop-accounting-buffer { radius-scheme radius-scheme-name | session-id
session-id | time-range start-time stop-time | user-name user-name }

View

Any view

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 80 characters.
Description

Using `display stop-accounting-buffer` command, you can 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` command.

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.

For the related commands, see `reset stop-accounting-buffer`, `stop-accounting-buffer enable`, `retry stop-accounting`.

Example

```bash
# Display the stopping accounting requests saved in the system buffer since 0:0:0 to 23:59:59 on August 31, 2002.
Total find 0 record
```

2.2.8 key

Syntax

```bash
key { accounting | authentication } string
undo key { accounting | authentication }
```

View

RADIUS scheme view

Parameter

- `accounting`: Configures to set/delete the encryption key for 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 “huawei”.

Huawei Technologies Proprietary
Description

Using **key** command, you can configure encryption key for RADIUS authentication/authorization or accounting packet. Using **undo key** command, you can restore the default key.

RADIUS client (switch system) and RADIUS server use MD5 algorithm to encrypt the exchanged packets. The two ends verify the packet through setting the encryption 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 encryption keys, you are supposed to set two encryption keys respectively.

For the related commands, see **primary accounting**, **primary authentication**, **radius scheme**.

Example

Example 1:

# Set the authentication/authorization key of the RADIUS scheme, huawei, to “hello”.

[Quidway-radius-huawei] key authentication hello

Example 2:

# Set the accounting packet key of the RADIUS scheme, huawei, to “ok”.

[Quidway-radius-huawei] key accounting ok

2.2.9 local-server

Syntax

```plaintext
local-server nas-ip ip-address key password
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 password**: Set password of logon user. *password* is a character string containing up to 16 characters.
Description

Using **local-server** command, you can configure the parameters of local RADIUS server. Using **undo local-server** command, you can cancel a local RADIUS server.

RADIUS service, which adopts authentication/authorization/accounting servers to manage users, is widely used in Quidway series switches. Besides, local authentication/authorization service is also used in these products and it is called local RADIUS function, i.e. realize basic RADIUS function on the switch.

---

⚠️ Caution:

- When using local RADIUS server function of Huawei, remember the number of UDP port used for authentication is 1645 and that for accounting is 1646.
- The password configured by this command must be the same as that of the RADIUS authentication/authorization packet configured by the command **key authentication** in RADIUS scheme view.

---

Quidway series switches support up to 16 local RADIUS authentication servers.

For the related commands, see **radius scheme**, **state** and **key**.

Example

```plaintext
# Set the IP address of local RADIUS authentication server to 10.110.1.2 and the password to huawei.
[Quidway] local-server nas-ip 10.110.1.2 key huawei
```

2.2.10 **nas-ip**

**Syntax**

```
nas-ip ip-address
undo nas-ip
```

**View**

RADIUS scheme view

**Parameter**

- **ip-address**: IP address in dotted decimal format.
Description

Using the `nas-ip` command, you can set the source IP address of the network access server (NAS, the switch in this manual), so that all packets destined for the RADIUS server carry the same source IP address. Using the `undo nas-ip` command, you can 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.

For the related command, see `display radius`, `radius nas-ip`.

Example

```
# Set the source IP address that is carried in the RADIUS packets sent by the NAS (the switch) to 10.1.1.1.
[Quidway] radius scheme test1
[Quidway-radius-test1] nas-ip 10.1.1.1
```

2.2.11 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`: UDP port number. ranging from 1 to 65535.

Description

Using `primary accounting` command, you can configure the IP address and port number for the primary accounting server. Using `undo primary accounting` command, you can 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.
After creating a RADIUS scheme, you are supposed to set IP addresses and UDP port numbers for the RADIUS servers, including primary/secondary authentication/authorization servers and accounting servers. In real networking environments, the above parameters shall be set according to the specific requirements. However, at least you have to set one authentication/authorization server and an accounting server. Besides, ensure that the RADIUS service port settings on the Ethernet switch is consistent with the port settings on the RADIUS server.

For the related commands, see key, radius scheme, state.

Example

```
# Set the IP address of the primary accounting server of RADIUS scheme, "huawei", to 10.110.1.2 and the UDP port 1813 to provide RADIUS accounting service.
[Quidway-radius-huawei] primary accounting 10.110.1.2 1813
```

### 2.2.12 primary authentication

**Syntax**

`primary authentication ip-address [ port-number ]`

`undo primary authentication`

**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**

Using `primary authentication` command, you can configure the IP address and port number for the primary RADIUS authentication/authorization. Using `undo primary authentication` command, you can restore the default IP address and port number of the primary RADIUS authentication/authorization.

By default, as 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; as for the "system" 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.

After creating a RADIUS scheme, you are supposed to set IP addresses and UDP port numbers for the RADIUS servers, including primary/secondary authentication/authorization servers and accounting servers. In real networking environments, the above parameters shall be set according to the specific
requirements. However, at least you have to set one authentication/authorization server and an accounting server. Besides, ensure that the RADIUS service port settings on the Ethernet switch is consistent with the port settings on the RADIUS server.

For the related commands, see key, radius scheme, state.

Example

# Set the IP address of the primary authentication/authorization server of RADIUS scheme, “huawei”, to 10.110.1.1 and the UDP port 1812 to provide RADIUS authentication/authorization service.

[Quidway-radius-huawei] primary authentication 10.110.1.1 1812

2.2.13 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

Using the radius nas-ip command, you can specify the source address of the RADIUS packet sent from NAS. Using the undo radius nas-ip command, you can 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

# Configure the switch to send RADIUS packets from 129.10.10.1.

[Quidway] radius nas-ip 129.10.10.1
2.2.14 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

Using radius scheme command, you can configure a RADIUS scheme and enter its view. Using undo radius scheme command, you can delete the specified RADIUS scheme.

By default, a RADIUS scheme named as system has been created in the system. Its attributes 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 system). So 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 server-groups, including the default scheme named as system.

Although undo radius scheme can remove a specified RADIUS scheme. However, the default one cannot be removed. Note that a scheme currently in use by the online user cannot be removed.

For the related commands, see 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

# Create a RADIUS scheme named “huawei” and enters its view.
[Quidway] radius scheme huawei
[Quidway-radius-huawei]
2.2.15 reset radius statistics

Syntax
reset radius statistics

View
User view

Parameter
None

Description
Using the reset radius statistics command, you can clear the statistic information related to the RADIUS protocol.

For the related command, see display radius.

Example

# Clear the RADIUS protocol statistics.
<Quidway> reset radius statistics

2.2.16 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 80 characters.

Description

Using reset stop-accounting-buffer command, you can 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.

For the related commands, see stop-accounting-buffer enable, retry stop-accounting, display stop-accounting-buffer.

Example

# Delete the stopping accounting requests saved in the system buffer by the user, user0001@huawei163.net.
<Quidway> reset stop-accounting-buffer user-name user0001@huawei163.net

# Delete the stopping accounting requests saved in the system buffer since 0:0:0 to 23:59:59 on August 31, 2002.

2.2.17 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

Using **retry** command, you can configure retransmission times of RADIUS request packet. Using **undo retry** command, you can restore the retransmission 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-times**, NAS considers the communication with the primary and secondary RADIUS servers has been disconnected.

Setting a suitable retry-time according to the network situation can speed up the system response.

For the related command, see **radius scheme**.

Example

```
# Set to retransmit the RADIUS request packet no more than 5 times for the RADIUS scheme huawei.
[Quidway-radius-huawei] retry 5
```

2.2.18 **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

Using **retry realtime-accounting** command, you can configure the maximum times of real-time accounting request failing to be responded. Using **undo retry realtime-accounting** command, you can restore the maximum times of real-time accounting request failing to be responded 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. Accordingly, it is necessary to
disconnect the user at NAS end and on RADIUS server synchronously when some unexpected failure occurs. Quidway Series Ethernet Switches support to set maximum times of real-time accounting request failing to be responded. NAS will disconnect the user if it has not received real-time accounting response from RADIUS server for some specified times.

How to calculate the value of count? 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.

For the related command, see **radius scheme**

**Example**

```
# Allow the real-time accounting request failing to be responded for up to 10 times.
[Quidway-radius-huawei] retry realtime-accounting 10
```

### 2.2.19 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**

Using **retry stop-accounting** command, you can configure the maximal retransmission times after stopping accounting request. Using **undo retry stop-accounting** command, you can 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.
For the related commands, see \texttt{reset stop-accounting-buffer}, \texttt{radius scheme}, \texttt{display stop-accounting-buffer}.

\textbf{Example}

\# Indicate that, when stopping accounting request for the RADIUS scheme “Huawei”,
\hspace{1em}the switch will retransmit the packets for up to 1000 times.
\[ \text{[Quidway-radius-huawei]} \text{ retry stop-accounting 1000} \]

\textbf{2.2.20 secondary accounting}

\textbf{Syntax}

\texttt{secondary accounting ip-address [ port-number ]}

\texttt{undo secondary accounting}

\textbf{View}

RADIUS scheme view

\textbf{Parameter}

\textit{ip-address}: IP address, in dotted decimal format. By default, the IP addresses of
\hspace{1em}second accounting server is at 0.0.0.0.

\textit{port-number}: Specifies the UDP port number, ranging from 1 to 65535. By default, the
\hspace{1em}accounting service is provided via UDP 1813.

\textbf{Description}

Using \texttt{secondary accounting} command, you can configure the IP address and port
\hspace{1em}number for the second RADIUS accounting server. Using \texttt{undo secondary}
\hspace{1em}accounting command, you can restore the IP address and port number to default
\hspace{1em}values.

For detailed information, read the Description of the \texttt{primary accounting} command.

For the related commands, see \texttt{key}, \texttt{radius scheme}, \texttt{state}.

\textbf{Example}

\# Set the IP address of the second accounting server of RADIUS scheme, huawei, to
\hspace{1em}10.110.1.1 and the UDP port 1813 to provide RADIUS accounting service.
\[ \text{[Quidway-radius-huawei]} \text{ secondary accounting 10.110.1.1 1813} \]

\textbf{2.2.21 secondary authentication}

\textbf{Syntax}

\texttt{secondary authentication ip-address [ port-number ]}

Huawei Technologies Proprietary

2-36
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

Using secondary authentication command, you can configure the IP address and port number for the second RADIUS authentication/authorization. Using undo secondary authentication command, you can restore the IP address and port number to default values.

For detailed information, read the Description of the primary authentication command.

For the related commands, see key, radius scheme, state.

Example

# Set the IP address of the second authentication/authorization server of RADIUS scheme, “huawei”, to 10.110.1.2 and the UDP port 1812 to provide RADIUS authentication/authorization service.

[Quidway-radius-huawei] secondary authentication 10.110.1.2 1812

2.2.22 server-type

Syntax

 server-type { huawei | iphotel | portal | standard }

 undo server-type

View

RADIUS scheme view

Parameter

 huawei: Configures the switch system to support the RADIUS server of Huawei type, which requires the RADIUS client end (switch system) and RADIUS server to interact according to the private RADIUS protocol regulation and packet format of Huawei Technologies Co., Ltd.
**iphotel**: Configures the switch system to support the RADIUS server of IP Hotel type, which requires the RADIUS client end (switch system) and RADIUS server to interact according to the regulation and packet format of IP Hotel (an extension of RADIUS protocol).

**portal**: Configures the switch system to support the RADIUS server of portal type, which requires the RADIUS client end (switch system) and RADIUS server to interact according to the regulation and packet format of Portal (an extension of RADIUS protocol).

**standard**: Configures the switch system to support the RADIUS server of Standard type, which requires the RADIUS client end (switch system) and RADIUS server to interact according to the regulation and packet format of standard RADIUS protocol (RFC 2138/2139 or newer).

**Description**

Using **server-type** command, you can configure the RADIUS server type supported by the switch. Using **undo server-type** command, you can restore the RADIUS server type to the default setting.

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 **huawei** type.

Quidway Series Ethernet Switches support standard RADIUS protocol and the extended RADIUS service platform developed by Huawei Technologies.

For the related command, see **radius scheme**.

**Example**

```bash
# Set RADIUS server type of RADIUS scheme, “huawei” to **huawei**.
[quidway-radius-huawei] server-type huawei
```

### 2.2.23 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**

Using **state** command, you can configure the state of RADIUS server.

By default, all the RADIUS servers in every RADIUS scheme 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.

For the related commands, see radius scheme, primary authentication, secondary authentication, primary accounting, secondary accounting.

**Example**

```
# Set the second authentication server of RADIUS scheme, “huawei”, to be active.
[Quidway-radius-huawei] state secondary authentication active
```

### 2.2.24 stop-accounting-buffer enable

**Syntax**

```plaintext
stop-accounting-buffer enable
undo stop-accounting-buffer enable
```

**View**

RADIUS scheme view

**Parameter**

None

**Description**

Using **stop-accounting-buffer enable** command, you can configure to save the stopping accounting requests without response in the switch system buffer. Using
undo stop-accounting-buffer enable command, you can cancel the function of saving the stopping accounting requests without response in the switch system buffer.

By default, enable to save the stopping accounting requests in the buffer. 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.

For the related commands, see reset stop-accounting-buffer, radius scheme, display stop-accounting-buffer.

Example

```bash
# Indicate that, for the RADIUS scheme "Huawei", the switch will save the stopping accounting request packets in the buffer
[Quidway-radius-huawei] stop-accounting-buffer enable
```

### 2.2.25 timer

#### Syntax

```plaintext
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

Using `timer` command, you can configure RADIUS server response timer. Using `undo timer` command, you can restore the default value of the timer.

After RADIUS (authentication/authorization or accounting) request packet has been transmitted for a period of time, if NAS has not received the response from 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 system. This command is used to set this timer.
Setting a suitable timer according to the network situation will enhance the system performance.

For the related commands, see radius scheme, retry.

Example

```
# Set the response timeout timer of RADIUS scheme, huawei, to 5 seconds.
[Quidway-radius-huawei] timer 5
```

2.2.26 timer quiet

Syntax

```
timer 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 servers switch over.

Use the `undo timer quiet` command to set the quiet time interval to its default value.

The functions of the quiet time interval are as follows:
- The switch sends RADIUS packets to the primary RADIUS server.
- If the switch affirms that the primary server does not respond, it then sends RADIUS packets to the secondary RADIUS server.
- 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

```
# Set the quiet time interval of the RADIUS scheme “RAserver” to 3 minutes.
[Quidway] radius scheme RAserver
[Quidway-radius-RAserver] timer quiet 3
```

2.2.27 timer realtime-accounting

Syntax

```
timer realtime-accounting minutes
```

Huawei Technologies Proprietary
undo timer realtime-accounting

View

RADIUS scheme view

Parameter

minutes: Real-time accounting interval, ranging from 3 to 60 and measured in minutes. By default, the value is 12. It must be a multiple of 3.

Description

Using `timer realtime-accounting` command, you can configure the real-time accounting interval. Using `undo timer realtime-accounting` command, you can 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>
<thead>
<tr>
<th>Number of users</th>
<th>Real-time accounting interval (minute)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 to 99</td>
<td>3</td>
</tr>
<tr>
<td>100 to 499</td>
<td>6</td>
</tr>
<tr>
<td>500 to 999</td>
<td>12</td>
</tr>
<tr>
<td>≥1000</td>
<td>≥15</td>
</tr>
</tbody>
</table>

For the related commands, see `retry realtime-accounting`, `radius scheme`.

Example

```
# Set the real-time accounting interval of RADIUS scheme, “huawei”, to 15 minutes.
[Quidway-radius-huawei] timer realtime-accounting 15
```

2.2.28 user-name-format

Syntax

```
user-name-format { with-domain | without-domain }
```

Huawei Technologies Proprietary
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

Using user-name-format command, you can configure the username format sent to RADIUS server.

By default, as for the newly created RADIUS scheme, the username sent to RADIUS servers includes an ISP domain name; as for the "system" RADIUS scheme created by the system, the username sent to RADIUS servers excludes 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 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 to be sent to RADIUS server carries ISP domain name or not.

Note:
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.)

For the related command, see radius scheme.

Example

# Specify to send the username without domain name to RADIUS server.

[Quidway-radius-huawei] user-name-format without-domain
Chapter 3  HABP Configuration Commands

3.1  HABP Commands

3.1.1  display debugging habp

Syntax

display debugging habp

View

Any view

Parameter

None

Description

Using the display debugging habp command, you can view HAMP debugging state.

Example

# Display HABP debugging state.

[Quidway] display debugging habp

HABP Debugging switch is on

3.1.2  display habp

Syntax

display habp

View

Any view

Parameter

None

Description

Using the display habp command, you can view configuration information and state of HABP attribute.
Example

# Display configuration information and state of HABP attribute.
[Quidway] display habp

Global HABP information:
  HABP Mode: Server
  Sending HABP request packets every 20 seconds
  Bypass VLAN: 2

Table 3-1 Display information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HABP Mode</td>
<td>HABP mode for the current switch, including server and client</td>
</tr>
<tr>
<td>Sending HABP request packets every 20 seconds</td>
<td>Time interval to send HABP request packets</td>
</tr>
<tr>
<td>Bypass VLAN</td>
<td>Send HABP packets in specified VLANs</td>
</tr>
</tbody>
</table>

3.1.3 display habp table

Syntax

display habp table

View

Any view

Parameter

None

Description

Using the display habp table command, you can view HABP MAC address table.

Example

# Display HABP MAC address table.
[Quidway] display habp table

MAC            Holdtime  Receive Port
001f-3c00-0030  53      Ethernet0/1
3.1.4 display habp traffic

Syntax

display habp traffic

View

Any view

Parameter

None

Description

Using the `display habp traffic` command, you can view HABP packet statistics.

Example

```bash
# Display HABP packet statistics.
[Quidway] display habp traffic
HABP counters :
   Packets output: 0, Input: 0
   ID error: 0, Type error: 0, Version error: 0
   Sent failed: 0
```

3.1.5 habp enable

Syntax

```
habp enable
undo habp enable
```

View

System view

Parameter

None

Description

Using the `habp enable` command, you can enable HABP attribute at a switch. Using the `undo habp enable` command, you can disable HABP attribute at a switch.

By default, HABP attribute is disabled at a switch.

If 802.1x attribute is enabled on switch and HABP attribute is not enabled, for those ports where 802.1x authentication is skipped, packets will be filtered by 802.1x attribute,
so the management over them is also impossible. When 802.1x attribute are enabled, HABP attribute should be enabled meanwhile.

Example

```
# Enable HABP attribute at a switch.
[Quidway] habp enable
```

### 3.1.6 habp server vlan

**Syntax**

```
habp server vlan vlan-id
undo habp server
```

**View**

System view

**Parameter**

*vlan-id*: VLAN ID, in range of 1~4094

**Description**

Using the `habp server vlan` command, you can set HABP mode as server and specify transmitting HABP packets in a specific VLAN. Using the `undo habp server vlan` command, you can restore the HABP mode to the default value.

By default, the HABP mode is client.

You must first enable HABP attribute at a switch using the `habp enable` command, and then specify HABP mode as server.

**Example**

```
# Specify HABP mode as server and transmit HABP packets in VLAN2.
[Quidway] habp server vlan 2
```

### 3.1.7 habp timer

**Syntax**

```
habp timer interval
undo habp timer
```

**View**

System view
Parameter

*interval*: Time interval to send HABP request packets, in range of 5~600 seconds. By default, the time interval is 20 seconds.

Description

Using the `habp timer` command, you can define time interval for a switch to send HABP request packet. Using the `undo habp timer` command, you can restore the time interval to the default value.

The command is only available on the switch whose HABP mode is set as server.

Example

# Define the time interval to send HABP request packets as 50 seconds.

[Quidway] habp timer 50
# Table of Contents

**Chapter 1 ARP Configuration Commands** .................................................................................. 1-1
  1.1 ARP Configuration Commands .......................................................................................... 1-1
    1.1.1 arp check enable ..................................................................................................... 1-1
    1.1.2 arp static .................................................................................................................. 1-1
    1.1.3 arp timer aging ........................................................................................................ 1-2
    1.1.4 debugging arp packet .............................................................................................. 1-3
    1.1.5 display arp ............................................................................................................... 1-4
    1.1.6 display arp timer aging ............................................................................................ 1-5
    1.1.7 reset arp .................................................................................................................. 1-6
  1.2 Gratuitous ARP Configuration Commands ........................................................................ 1-6
    1.2.1 gratuitous-arp-learning enable ................................................................................ 1-6

**Chapter 2 DHCP-Snooping Configuration Commands** ............................................................. 2-1
  2.1 DHCP-Snooping Configuration Commands ...................................................................... 2-1
    2.1.1 dhcp-snooping ......................................................................................................... 2-1
    2.1.2 dhcp-snooping trust ................................................................................................. 2-1
    2.1.3 display dhcp-snooping ............................................................................................ 2-2
    2.1.4 display dhcp-snooping count ................................................................................... 2-3
    2.1.5 display dhcp-snooping trust .................................................................................... 2-3

**Chapter 3 DHCP Client Configuration Commands** .................................................................. 3-1
  3.1 DHCP Client Configuration Commands ............................................................................ 3-1
    3.1.1 debugging dhcp client ............................................................................................. 3-1
    3.1.2 display dhcp client ................................................................................................... 3-1
    3.1.3 ip address dhcp-alloc .............................................................................................. 3-2

**Chapter 4 BOOTP Client Configuration Commands** ................................................................. 4-1
  4.1.1 debugging bootp client .............................................................................................. 4-1
  4.1.2 display bootp client .................................................................................................. 4-1
  4.1.3 ip address bootp-alloc ............................................................................................. 4-2

**Chapter 5 Access Management Configuration Commands** .................................................... 5-1
  5.1 Access Management Configuration Commands ............................................................... 5-1
    5.1.1 am enable ................................................................................................................ 5-1
    5.1.2 am isolate ................................................................................................................ 5-1
    5.1.3 am user-bind ............................................................................................................ 5-2
    5.1.4 display am ............................................................................................................... 5-3
    5.1.5 display am user-bind ............................................................................................... 5-4

**Chapter 6 IP Performance Configuration Commands** ............................................................ 6-1
  6.1 IP Performance Configuration Commands ......................................................................... 6-1
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1.1 display fib</td>
<td>6-1</td>
</tr>
<tr>
<td>6.1.2 display icmp statistics</td>
<td>6-2</td>
</tr>
<tr>
<td>6.1.3 display ip socket</td>
<td>6-3</td>
</tr>
<tr>
<td>6.1.4 display ip statistics</td>
<td>6-5</td>
</tr>
<tr>
<td>6.1.5 display tcp statistics</td>
<td>6-6</td>
</tr>
<tr>
<td>6.1.6 display tcp status</td>
<td>6-8</td>
</tr>
<tr>
<td>6.1.7 reset ip statistics</td>
<td>6-8</td>
</tr>
<tr>
<td>6.1.8 reset tcp statistics</td>
<td>6-9</td>
</tr>
<tr>
<td>6.1.9 tcp timer fin-timeout</td>
<td>6-9</td>
</tr>
<tr>
<td>6.1.10 tcp timer syn-timeout</td>
<td>6-10</td>
</tr>
<tr>
<td>6.1.11 tcp window</td>
<td>6-11</td>
</tr>
</tbody>
</table>
Chapter 1 ARP Configuration Commands

1.1 ARP Configuration Commands

1.1.1 arp check enable

Syntax

arp check enable
undo arp check enable

View

System view

Parameter

None

Description

Using `arp check enable` command, you can enable the checking of ARP entry, that is, the device does not learn the ARP entry where the MAC address is multicast MAC address. Using `undo arp check enable` command, you can disable the checking of ARP entry, that is, the device learns the ARP entry where the MAC address is multicast MAC address.

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

Example

# Configure that the device learns the ARP entry where the MAC address is multicast MAC address.
[Quidway] undo arp check enable

1.1.2 arp static

Syntax

arp static ip-address mac-address [ vlan-id { interface-type interface-number | interface-name } ]
undo arp ip-address

Example

# Configure that the device learns the ARP entry where the MAC address is multicast MAC address.
[Quidway] undo arp check enable
System view

Parameter

- **ip-address**: IP address of the ARP mapping entry.
- **mac-address**: MAC address of ARP mapping entry, whose format is H-H-H (H indicates a hexadecimal number).
- **vlan-id**: VLAN to which the static ARP entry belongs, which is in the range of 1 to 4094.
- **interface-name**: Port to which the static ARP entry belong, represented with **interface-name**= **interface-type** **interface-number**, **interface-type** is port type and **interface-number** is port number. For details about **interface-type**, **interface-number** and **interface-name**, refer to the **Port Command Manual**.

Description

Using **arp static** command, you can configure the static ARP mapping entries in an ARP mapping table. Using **undo arp static** command, you can cancel a static ARP mapping entry from the ARP table.

By default, the mapping table of the system ARP is empty and the switch can maintain its address mapping by means of dynamic ARP.

Note that:

- Static ARP map entry will be always valid as long as Ethernet switch works normally. But if the VLAN corresponding ARP mapping entry is deleted, the ARP mapping entry will be also deleted. The valid period of dynamic ARP map entries will last only 20 minutes by default.
- The parameter **vlan-id** must be the ID of a VLAN that has been created by the user, and the Ethernet port specified behind this parameter must belong to the VLAN.

For the related command, see **reset arp**, **display arp**, **debugging arp**.

Example

```
# Associate the IP address 202.38.10.2 with the MAC address 00e0-fc01-0000, and the ARP mapping entry belongs to the Ethernet port Ethernet0/1 on VLAN1.
[Quidway] arp static 202.38.10.2 00e0-fc01-0000 1 ethernet0/1
```

### 1.1.3 arp timer aging

**Syntax**

```
arp timer aging aging-time
undo arp timer aging
```

Huawei Technologies Proprietary
### View

System view

### Parameter

**aging-time**: Aging time of dynamic ARP aging timer, which is in the range of 1 to 1440 minutes. By default, the aging time is 20 minutes.

### Description

Using **arp timer aging** command, you can configure the dynamic ARP aging timer. Using **undo arp timer aging** command, you can restore the default dynamic ARP aging time.

For the related command, see **display arp timer aging**.

### Example

```
# Configure the dynamic ARP aging timer to 10 minutes.
[Quidway] arp timer aging 10
```

#### 1.1.4 debugging arp packet

### Syntax

```
debugging arp packet
undo debugging arp packet
```

### View

User view

### Parameter

None

### Description

Using **debugging arp packet** command, you can enable ARP debugging. Using **undo debugging arp packet** command, you can disable the corresponding ARP debugging.

By default, undo ARP debugging is enabled.

For the related command, see **arp static, display arp**.

### Example

```
# Enable ARP packet debugging.
<Quidway> debugging arp packet
*0.771346-ARP-8-S1-arp_send:Send an ARP Packet, operation : 1,
sender_eth_addr :
```

Huawei Technologies Proprietary
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 1-1 Output description of the debugging arp packet display

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>operation</td>
<td>Kind of ARP packets: 1 ARP request packet; 2 ARP reply packet</td>
</tr>
<tr>
<td>sender_eth_addr</td>
<td>Ethernet address of the sender</td>
</tr>
<tr>
<td>sender_ip_addr</td>
<td>IP address of the sender</td>
</tr>
<tr>
<td>target_eth_addr</td>
<td>Target Ethernet address. If the packet is ARP request packet, the target IP address will be 0</td>
</tr>
<tr>
<td>target_ip_addr</td>
<td>Target IP address</td>
</tr>
</tbody>
</table>

1.1.5 display arp

Syntax

display arp [ dynamic | static | ip-address ]

View

Any view

Parameter

dynamic: Display the dynamic ARP entries in ARP mapping table.
static: Display the static ARP entries in ARP mapping table.

ip-address: Display ARP mapping entries according to specified IP address.

Description

Using display arp command, you can view the ARP mapping table.

For the related command, see arp static, reset arp, debugging arp.

Example

# Display all the ARP entries.
<Quidway> display arp
### Table 1-2 Output description of the display arp display

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>IP address of the ARP mapping entry</td>
</tr>
<tr>
<td>MAC Address</td>
<td>MAC address of the ARP mapping entry</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>VLAN to which the static ARP entry belongs</td>
</tr>
<tr>
<td>Port Name</td>
<td>Port to which the static ARP entry belongs</td>
</tr>
<tr>
<td>Aging</td>
<td>Aging time of dynamic ARP entry in minutes</td>
</tr>
<tr>
<td>Type</td>
<td>Type of ARP entry</td>
</tr>
</tbody>
</table>

#### 1.1.6 display arp timer aging

**Syntax**

```plaintext
display arp timer aging
```

**View**

Any view

**Parameter**

```
vlan-id: VLAN interface.
```

**Description**

Using `display arp timer aging` command, you can view the current setting of the dynamic ARP map aging timer.

For the related command, see `arp timer aging`.

**Example**

```
# Display the current setting of the ARP map aging timer.
[Quidway] display arp timer aging
Current ARP aging time is 10 minute(s)
```
1.1.7 reset arp

Syntax

```
reset arp [ dynamic | static | interface { interface-type interface-number | interface-name } ]
```

View

User view

Parameter

- **dynamic**: Clear the dynamic ARP mapping entries.
- **static**: Clear the static ARP mapping entries
- **interface interface-name**: Clear the ARP mapping entries that are related to the specified port, represented with `interface-name= interface-type interface-number`. `interface-type` is port type and `interface-number` is port number. For details about `interface-type`, `interface-number` and `interface-name`, refer to the Port Command Manual.

Description

Using `reset arp` command, you can reset the ARP mapping entries.

For the related command, see `arp static, display arp`.

Example

```
# Reset the static ARP entries.
<Quidway> reset arp static
```

1.2 Gratuitous ARP Configuration Commands

1.2.1 gratuitous-arp-learning enable

Syntax

```
gratuitous-arp-learning enable
undo gratuitous-arp-learning enable
```

View

System view

Parameter

None
Description

Use the `gratuitous-arp-learning enable` command to enable gratuitous ARP packet learning.

Use the `undo gratuitous-arp-learning enable` command to disable this function.

By default, gratuitous ARP packet learning is disabled.

Gratuitous ARP function is to implement the following functions by sending out gratuitous ARP packets:

- By sending gratuitous ARP packets, network devices can figure out whether the IP addresses of other devices conflict with its own.
- If the device which sends the gratuitous ARP packet changed its hardware address (probably, it turns off, has its interface card changed, and then reboots), this packet can make old hardware address in the cache of other devices update accordingly.

Related command: `debugging arp packet`.

Example

# Enable gratuitous ARP packet learning on the switch Quidway A.

```
<QuidwayA> system-view
System View: return to User View with Ctrl+Z.
[QuidwayA] gratuitous-arp-learning enable
```
Chapter 2  DHCP-Snooping Configuration

Commands

2.1  DHCP-Snooping Configuration Commands

2.1.1  dhcp-snooping

Syntax

dhcp-snooping
undo dhcp-snooping

View

System view

Parameter

None

Description

Using dhcp-snooping command, you can enable DHCP-Snooping function on the switch to record users' IP addresses. Using undo dhcp-snooping command, you can disable this function.

By default, The switch is disabled to listen to DHCP broadcast packets and record users' IP addresses.

For the related command, see display dhcp-snooping.

Example

# Enable DHCP-Snooping.
[Quidway] dhcp-snooping

2.1.2  dhcp-snooping trust

Syntax

dhcp-snooping trust
undo dhcp-snooping trust
View

Ethernet port view

Parameter

None

Description

Using `dhcp-snooping trust` command, you can configure a trusted port. Using `undo dhcp-snooping trust` command, you can restore the trusted port as distrusted.

By default, the switch ports are set as distrusted.

For the related command, see `display dhcp-snooping trust`.

Example

```
# Configure Ethernet0/1 as a trusted port.
[Quidway-Ethernet0/1] dhcp-snooping trust
```

2.1.3  `display dhcp-snooping`

Syntax

`display dhcp-snooping [ vlan { vlan_list | all } ]`

View

Any view

Parameter

`vlan { vlan_list | all }`: Displays DHCP-Snooping binding information of a specified VLAN, where `vlan_list = { vlan_id [ to vlan_id ]}<1-10> &<1-10>` and `vlan_id` is in the range of 1 to 4094; `&<1-10>` means that you can repeat the parameters before for ten times at most. `all` represents all VLANs.

Description

Using `display dhcp-snooping` command, you can view the DHCP-Snooping correspondence table, which include these items: Binding type, IP address the DHCP server assigns to the user, MAC address of the user, lease time of the IP address, interface through which the user connects to the switch, and the VLAN that interface belongs to.

For the related command, see `dhcp-snooping`.

Example

```
# Display DHCP-Snooping binding information.
<Quidway> display dhcp-snooping
```

Huawei Technologies Proprietary
<table>
<thead>
<tr>
<th>Type</th>
<th>IP Address</th>
<th>MAC Address</th>
<th>Lease VLAN</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>dynamic</td>
<td>202.38.12.45</td>
<td>00e0-fc00-0006</td>
<td>286</td>
<td>Ethernet0/1</td>
</tr>
</tbody>
</table>

### 2.1.4 display dhcp-snooping count

**Syntax**

```
display dhcp-snooping count
```

**View**

Any view

**Parameter**

None

**Description**

Use the `display dhcp-snooping count` command to display the number of the DHCP-Snooping entries in the binding table.

**Example**

```
# Display the number of the DHCP-Snooping entries in the binding table.
<Quidway> display dhcp-snooping count
0 dhcp-snooping item(s) found
```

### 2.1.5 display dhcp-snooping trust

**Syntax**

```
display dhcp-snooping trust
```

**View**

Any view

**Parameter**

None

**Description**

Using `display dhcp-snooping trust` command, you can view the status of the DHCP-Snooping function and the information about the trusted ports.

For the related command, see `dhcp-snooping trust`. 
Example

# Display the status of the DHCP-Snooping function and the information about the trusted ports.
<Quidway> display dhcp-snooping trust
dhcp-snooping is enabled
dhcp-snooping trust become effective

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trusted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet0/1</td>
<td>Trusted</td>
</tr>
</tbody>
</table>
Chapter 3  DHCP Client Configuration Commands

3.1  DHCP Client Configuration Commands

3.1.1  debugging dhcp client

**Syntax**

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

**View**

User view

**Parameter**

- **all**: All DHCP client debugging.
- **error**: DHCP client error (including packet unrecognizable) debugging.
- **event**: DHCP client event (including address allocation and data update) debugging.
- **packet**: DHCP client packet debugging.

**Description**

Using the `debugging dhcp client` command, you can enable DHCP client debugging. Using the `undo debugging dhcp client` command, you can disable DHCP client debugging.

By default, all DHCP client debugging is disabled.

**Example**

```
# Enable DHCP client event debugging.
<Quidway> debugging dhcp client event
```

3.1.2  display dhcp client

**Syntax**

```
display dhcp client [ verbose ]
```

**View**

Any view
### Parameter

**verbose**: Displays detailed information about address allocation at DHCP client.

### Description

Using the `display dhcp client` command, you can view detailed information about address allocation at DHCP client.

### Example

```bash
# Display detailed information about address allocation at DHCP client.
[Quidway] 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: huawei.com
Client ID: HUAWEI-00e0.fc0a.c3ef-Ethernet0/0
Next timeout will happen after 0 days 11 hours 56 minutes 1 seconds.
```

#### 3.1.3 ip address dhcp-alloc

### Syntax

```
ip address dhcp-alloc
undo ip address dhcp-alloc
```

### View

VLAN interface view

### Parameter

None

### Description

Using the `ip address dhcp-alloc` command, you can configure VLAN interface to obtain IP address using DHCP. Using the `undo ip address dhcp-alloc` command, you can remove the configuration.

By default, the VLAN interface does not obtain IP address using DHCP.
Example

# Configure VLAN interface to obtain IP address using DHCP.

[Quidway-Vlan-interface1] ip address dhcp-alloc
Chapter 4  BOOTP Client Configuration Commands

4.1.1 debugging bootp client

Syntax

default debugging bootp client
undo debugging bootp client

View

User view

Parameter

None

Description

Using the debugging bootp client command, you can enable BOOTP client debugging. Using the undo debugging bootp client command, you can disable BOOTP client debugging.

By default, BOOTP client debugging is disabled.

Example

# Enable BOOTP client debugging.
<Quidway> debugging bootp client

4.1.2 display bootp client

Syntax

display bootp client [ interface vlan-interface vlan-id ]

View

Any view

Parameter

vlan-id: VLAN interface ID.

vlan-interface vlan_id: Display BOOTP client information of specified VLAN interface.

Description
Using the **display bootp client** command, you can view the information about BOOTP client, including its MAC address and the applied IP address etc.

**Example**

```bash
# Display the information about BOOTP client.
[Quidway] display bootp client interface vlan-interface 1
Vlan-interface1:
Allocated IP: 169.254.0.2 255.255.0.0
Transaction ID = 0x3d8a7431
Mac Address  00e0-fc0a-c3ef
```

**Table 4-1 Display information description of display bootp client**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan-interface1</td>
<td>Configure VLAN interface 1 to obtain IP address using BOOTP</td>
</tr>
<tr>
<td>Transaction ID</td>
<td>XID filed value in BOOTP packet</td>
</tr>
</tbody>
</table>

**4.1.3 ip address bootp.alloc**

**Syntax**

```plaintext
ip address bootp-alloc
undo ip address bootp-alloc
```

**View**

VLAN interface view/M-Ethernet port view

**Parameter**

None

**Description**

Using the **ip address bootp-alloc** command, you can configure VLAN interface to obtain IP address using BOOTP. Using the **undo ip address bootp-alloc** command, you can remove the configuration.

By default, the VLAN interface does not obtain IP address using BOOTP.

For the related command, see **display bootp client**.

**Example**

```bash
# Configure VLAN interface 1 to obtain IP address using BOOTP.
[Quidway-Vlan-interface1] ip address bootp-alloc
```
Chapter 5  Access Management Configuration Commands

5.1  Access Management Configuration Commands

5.1.1  am enable
Syntax
   am enable
   undo am enable
View
   System view
Parameter
   None
Description
   Using am enable command, you can enable the access management function. Using undo am enable command, you can disable the function.
   By default, Access management function disabled.
   When using the access management function, It is recommended to cancel the static ARP configuration to ensure that the binding of IP address and Ethernet switch take effect. If you have configured the static ARP for an IP address in the current port IP address pool from some other port, the system will prompt to cancel the static ARP setting.

Example
   # Enable the access management function.
   [Quidway] am enable

5.1.2  am isolate
Syntax
   am isolate interface-list
   undo am isolate interface-list
Parameter

interface-list: Specifies a list of ports isolated from the specified port in the
{ { interface-type interface-number | interface-name } [ to { interface-type interface-number | interface-name } ] } &<1-10> format. interface-name: Specified the
port name, represented with interface-name= interface-type interface-number.
interface-type is port type and interface-number is port number. For details about
interface-type, interface-number and interface-name, refer to the Port Command
Manual. &<1-10> indicates the preceding parameter can be input up to 10 times.

Description

Using am isolate command, you can configure Layer 2 isolation on a port so as to
prevent the packets from being forwarded on Layer 2 between the specified port and
some other port (group). Using undo am isolate command, you can cancel the Layer 2
isolation on the port.

By default, The isolation port pool is null and the packets are allowed to be forwarded
between the specified port and all other ports on Layer 2.

The port isolation is bidirectional. Isolating the port itself does not make any sense.

Example

# Isolate Ethernet0/1 from Ethernet0/2, and Ethernet0/4 through Ethernet0/7.
[Quidway-Ethernet0/1] am isolate ethernet0/2 ethernet 0/4 to ethernet 0/7

5.1.3 am user-bind

Syntax

am user-bind { interface { interface-name | interface-type interface-number } 
{ mac-addr mac | ip-addr ip }* | mac-addr mac { interface { interface-name | interface-type interface-number } | ip-addr ip }* | ip-addr ip { interface { interface-name | interface-type interface-number } | mac-addr mac }* 
undo am user-bind { interface { interface-name | interface-type interface-number } 
{ mac-addr mac | ip-addr ip }* | mac-addr mac { interface { interface-name | interface-type interface-number } | ip-addr ip }* | ip-addr ip { interface { interface-name | interface-type interface-number } | mac-addr mac }* 

View

System view
Parameter

interface-name: Specifies the port name in the interface-name= interface-type interface-number format. interface-type: Specifies the port type. interface-number: Specifies the port number. For parameter description, refer to the interface command.

mac: MAC address.

ip: IP address.

Description

Using am user-bind command, you can bind port, IP address and MAC address. Using undo am user-bind command, you can remove the binding of port, IP address and MAC address binding.

Note that:

- One MAC address or one IP address cannot be bound more than once.
- The maximum binding number is 128.
- Do not perform "Port+IP+MAC" and "Port+IP" on the same port.

Example

# Bind port Ethernet0/1 and IP address 192.10.1.1.
[Quidway] am user-bind interface ethenet0/1 ip-addr 192.10.1.1

5.1.4 display am

Syntax

display am [ interface-list ]

View

Any view

Parameter

interface-list: Specifies a list of ports isolated from the specified port in the { { interface-type interface-number | interface-name } [ to { interface-type interface-number | interface-name } ] } &<1-10> format. interface-name: Specified the port name, represented with interface-name= interface-type interface-number. interface-type is port type and interface-number is port number. For details about interface-type, interface-number and interface-name, refer to the Port Command Manual. &<1-10> indicates the preceding parameter can be input up to 10 times.

Description

Using display am command, you can view the current access management configurations on part or all of the ports.
Example

# Display the access management configurations on Ethernet0/1 and Ethernet0/2.
<Quidway> 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 5-1 Description of information generated by the command display am

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet</td>
<td>Port to be displayed</td>
</tr>
<tr>
<td>Status</td>
<td>AM state on the port: enabled or disabled</td>
</tr>
<tr>
<td>IP Pools</td>
<td>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</td>
</tr>
<tr>
<td>Isolate Ports</td>
<td>Isolate ports. NULL represents no configuration</td>
</tr>
</tbody>
</table>

5.1.5 display am user-bind

Syntax

display am user-bind [ interface { interface-name | interface-type interface-number } ] | mac-addr mac | ip-addr ip ]

View

Any view

Parameter

interface-name: Specifies the port name in the interface-name= interface-type interface-number format. interface-type: Specifies the port type. interface-number: Specifies the port number. For parameter description, refer to the interface command.
mac: MAC address.
ip: IP address.
Description

Using **display am user-bind** command, you can view Port, IP address and MAC address binding information.

Example

# Display binding information of Ethernet0/1 port.

```
<Quidway> display am user-bind interface ethernet0/1

<table>
<thead>
<tr>
<th>Mac</th>
<th>IP</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>NULL</td>
<td>129.10.1.1</td>
<td>Ethernet0/1</td>
</tr>
</tbody>
</table>
```
Chapter 6  IP Performance Configuration Commands

6.1  IP Performance Configuration Commands

6.1.1  display fib

Syntax

display fib

View

Any view

Parameter

None

Description

Using display fib command, you can view the summary of the Forwarding Information Base. The information includes: destination address/mask length, next hop, current flag and outbound interface.

Example

# Display the summary of the Forwarding Information Base.
<Quidway> display fib

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Nexthop</th>
<th>Flag</th>
<th>TimeStamp</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>127.0.0.0/8</td>
<td>127.0.0.1</td>
<td>U</td>
<td>t[0]</td>
<td>InLoopBack0</td>
</tr>
</tbody>
</table>
Table 6-1 Description of the output information of the display fib command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flag</td>
<td>The flag options include:</td>
</tr>
<tr>
<td></td>
<td>B – Blackhole route</td>
</tr>
<tr>
<td></td>
<td>D – Dynamic route</td>
</tr>
<tr>
<td></td>
<td>G – Gateway route</td>
</tr>
<tr>
<td></td>
<td>H – Local host route</td>
</tr>
<tr>
<td></td>
<td>S – Static route</td>
</tr>
<tr>
<td></td>
<td>U – Route in UP status</td>
</tr>
<tr>
<td></td>
<td>R – Unreachable route</td>
</tr>
<tr>
<td></td>
<td>L – Route generated by ARP or ESIS</td>
</tr>
</tbody>
</table>

6.1.2 display icmp statistics

Syntax

display icmp statistics

View

Any view

Parameter

None

Description

Using display icmp statistics command, you can view the statistics information about ICMP packets.

For the related command, see display ip interface vlan-interface, reset ip statistics.

Example

# View statistics about ICMP packets.
<Quidway> 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           |
Table 6-2 Description of the output information of the `display icmp statistics` command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bad formats</td>
<td>Number of input packets in bad format</td>
</tr>
<tr>
<td>bad checksum</td>
<td>Number of input packets with wrong checksum</td>
</tr>
<tr>
<td>echo</td>
<td>Number of input/output echo request packets</td>
</tr>
<tr>
<td>destination unreachable</td>
<td>Number of input/output packets with unreachable destination</td>
</tr>
<tr>
<td>source quench</td>
<td>Number of input/output source quench packets</td>
</tr>
<tr>
<td>redirects</td>
<td>Number of input/output redirected packets</td>
</tr>
<tr>
<td>echo reply</td>
<td>Number of input/output echo reply packets</td>
</tr>
<tr>
<td>parameter problem</td>
<td>Number of input/output packets with parameter problem</td>
</tr>
<tr>
<td>timestamp</td>
<td>Number of input/output timestamp packets</td>
</tr>
<tr>
<td>information request</td>
<td>Number of input information request packets</td>
</tr>
<tr>
<td>mask requests</td>
<td>Number of input/output mask request packets</td>
</tr>
<tr>
<td>mask replies</td>
<td>Number of input/output mask reply packets</td>
</tr>
<tr>
<td>information reply</td>
<td>Number of output information reply packets</td>
</tr>
<tr>
<td>time exceeded</td>
<td>Number of time exceeded packets</td>
</tr>
</tbody>
</table>

### 6.1.3 display ip socket

**Syntax**

```plaintext
display ip socket [ socktype sock-type ] [ task-id socket-id ]
```

**View**

Any view

**Parameter**

`sock-type`: The type of a socket: (tcp:1, udp 2, raw ip 3).
task-id: The ID of a task, with the value ranging from 1 to 100.

socket-id: The ID of a socket, with the value ranging from 0 to 3072.

Description

Using the `display ip socket` command, you can display the information about the sockets in the current system.

Example

# Display the information about the socket of TCP type.

```plaintext
<Quidway> 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,
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,
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 6-3 Output description of the `display ip socket` display

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOCK_STREAM</td>
<td>The socket type</td>
</tr>
<tr>
<td>Task</td>
<td>The ID of a task</td>
</tr>
<tr>
<td>socketid</td>
<td>The ID of a socket</td>
</tr>
<tr>
<td>Proto</td>
<td>The protocol number used by the socket</td>
</tr>
<tr>
<td>sndbuf</td>
<td>The sending buffer size of the socket</td>
</tr>
<tr>
<td>rcvbuf</td>
<td>The receiving buffer size of the socket</td>
</tr>
<tr>
<td>sb_cc</td>
<td>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</td>
</tr>
</tbody>
</table>

Huawei Technologies Proprietary
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rb_cc</td>
<td>The current data size in the receiving buffer</td>
</tr>
<tr>
<td>socket option</td>
<td>The option of the socket</td>
</tr>
<tr>
<td>socket state</td>
<td>The state of the socket</td>
</tr>
</tbody>
</table>

## 6.1.4 display ip statistics

**Syntax**

```markdown
display ip statistics
```

**View**

Any view

**Parameter**

None

**Description**

Using `display ip statistics` command, you can view the statistics information about IP packets.

For the related command, see `display ip interface vlan-interface`, `reset ip statistics`.

**Example**

```bash
# View statistics about IP packets.
<Quidway> 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 6-4 Description of the output information of the `display ip statistics` command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sum</td>
<td>Sum of input packets</td>
</tr>
<tr>
<td>local</td>
<td>Number of received packets whose destination is the local device</td>
</tr>
<tr>
<td>bad protocol</td>
<td>Number of packets with wrong protocol number</td>
</tr>
<tr>
<td>bad format</td>
<td>Number of packets in bad format</td>
</tr>
<tr>
<td>bad checksum</td>
<td>Number of packets with wrong checksum</td>
</tr>
<tr>
<td>bad options</td>
<td>Number of packets that has wrong options</td>
</tr>
<tr>
<td>forwarding</td>
<td>Number of forwarded packets</td>
</tr>
<tr>
<td>local</td>
<td>Number of packets that are sent by the local device</td>
</tr>
<tr>
<td>dropped</td>
<td>Number of dropped packets during transmission</td>
</tr>
<tr>
<td>no route</td>
<td>Number of packets that cannot be routed</td>
</tr>
<tr>
<td>compress fails</td>
<td>Number of packets that cannot be compressed</td>
</tr>
<tr>
<td>input</td>
<td>Number of input fragments</td>
</tr>
<tr>
<td>output</td>
<td>Number of output fragments</td>
</tr>
<tr>
<td>dropped</td>
<td>Number of dropped fragments</td>
</tr>
<tr>
<td>fragmented</td>
<td>Number of packets that are fragmented</td>
</tr>
<tr>
<td>couldn't fragment</td>
<td>Number of packets that cannot be fragmented</td>
</tr>
<tr>
<td>sum</td>
<td>Number of packets that are reassembled</td>
</tr>
<tr>
<td>timeouts</td>
<td>Number of packets that time out</td>
</tr>
</tbody>
</table>

6.1.5 `display tcp statistics`

**Syntax**

`display tcp statistics`

**View**

Any view

**Parameter**

None
Description

Using `display tcp statistics` command, you can 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. And each kind of packets are 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 these displayed information are measured in packet.

For the related commands, see `display tcp status`, `reset tcp statistics`.

Example

```bash
# View statistics about TCP packets.
[Quidway]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: 0, connection disconnected: 0
  Initiated connections: 0, accepted connections: 0, established connections: 0
```

Huawei Technologies Proprietary

6-7
6.1.6 display tcp status

Syntax

display tcp status

View

Any view

Parameter

None

Description

Using **display tcp status** command, you can view the TCP connection state.

Example

```
# Display the state of all TCP connections.
<Quidway> 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  Established
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Add: port</td>
<td>Local IP address: local port</td>
</tr>
<tr>
<td>Foreign Add: port</td>
<td>Remote IP address: remote port</td>
</tr>
<tr>
<td>State</td>
<td>State of the TCP link</td>
</tr>
</tbody>
</table>

6.1.7 reset ip statistics

Syntax

reset ip statistics

View

User view

Parameter

None
Description

Using \texttt{reset ip statistics} command, you can reset the IP statistics information.

For the related commands, see \texttt{display ip interface vlan-interface}, \texttt{display ip statistics}.

Example

\begin{verbatim}
# Reset the IP statistics information.
<Quidway> reset ip statistics
\end{verbatim}

6.1.8 \texttt{reset tcp statistics}

Syntax

\texttt{reset tcp statistics}

View

User view

Parameter

None

Description

Using \texttt{reset tcp statistics} command, you can reset the TCP statistics information.

For the related command, see \texttt{display tcp statistics}.

Example

\begin{verbatim}
# Reset the TCP statistics information.
<Quidway> reset tcp statistics
\end{verbatim}

6.1.9 \texttt{tcp timer fin-timeout}

Syntax

\texttt{tcp timer fin-timeout \textit{time-value}}

\texttt{undo tcp timer fin-timeout}

View

System view

Parameter

\textit{time-value}: TCP finwait timer value in second, with the value ranging from 76 to 3600; By default, 675 seconds.
Description

Using `tcp timer fin-timeout` command, you can configure the TCP finwait timer. Using `undo tcp timer fin-timeout` command, you can restore the default value of the TCP finwait timer.

When the TCP connection state changes from `FIN_WAIT_1` to `FIN_WAIT_2`, the finwait timer is enabled. If the switch does not receive FIN packet before finwait timer timeouts, the TCP connection will be terminated.

For the related command, see `tcp timer syn-timeout`, `tcp window`.

Example

```bash
# Configure the TCP finwait timer value as 800 seconds.
[Quidway] tcp timer fin-timeout 800
```

6.1.10 tcp timer syn-timeout

Syntax

```
tcp timer syn-timeout time-value
undo tcp timer syn-timeout
```

View

System view

Parameter

`time-value`: TCP synwait timer value measured in second, whose value ranges from 2 to 600. The default `time-value` is 75 seconds.

Description

Using `tcp timer syn-timeout` command, you can configure the TCP synwait timer. Using `undo tcp timer syn-timeout` command, you can 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.

For the related command, see `tcp timer fin-timeout`, `tcp window`.

Example

```bash
# Configure the TCP synwait timer value as 80 seconds.
[Quidway] tcp timer syn-timeout 80
```
6.1.11  tcp window

Syntax

    tcp window window-size
    undo tcp window

View

    System view

Parameter

    window-size: 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 8KB.

Description

    Using tcp window command, you can configure the size of the transmission and receiving buffers of the connection-oriented Socket. Using undo tcp window command, you can restore the default size of the buffer.

    For the related command, see tcp timer fin-timeout, tcp timer syn-timeout.

Example

    # Configure the size of the transmission and receiving buffers as 3KB.
    [Quidway] tcp window 3
Table of Contents

Chapter 1 File System Management Commands .............................................................. 1-1
  1.1 File System ............................................................................................................... 1-1
      1.1.1 cd.................................................................................................................... 1-1
      1.1.2 copy............................................................................................................... 1-1
      1.1.3 delete............................................................................................................. 1-2
      1.1.4 dir ................................................................................................................. 1-3
      1.1.5 file prompt................................................................................................. 1-4
      1.1.6 format ........................................................................................................... 1-5
      1.1.7 mkdir............................................................................................................ 1-5
      1.1.8 more ............................................................................................................ 1-6
      1.1.9 move............................................................................................................. 1-6
      1.1.10 pwd............................................................................................................ 1-8
      1.1.11 rename ....................................................................................................... 1-8
      1.1.12 reset recycle-bin...................................................................................... 1-9
      1.1.13 rmdir ....................................................................................................... 1-10
      1.1.14 undelete.................................................................................................. 1-10
  1.2 Configuration File Management Commands ....................................................... 1-12
      1.2.1 reset saved-configuration ........................................................................... 1-12
      1.2.2 save.............................................................................................................. 1-13
  1.3 FTP Server Configuration Commands ................................................................ 1-13
      1.3.1 display ftp-server ....................................................................................... 1-13
      1.3.2 display ftp-user ......................................................................................... 1-14
      1.3.3 ftp server .................................................................................................. 1-14
      1.3.4 ftp timeout ............................................................................................... 1-15
      1.3.5 local-user .................................................................................................. 1-16
      1.3.6 password .................................................................................................. 1-16
      1.3.7 service-type .............................................................................................. 1-17
  1.4 FTP Client Commands ......................................................................................... 1-18
      1.4.1 ascii ............................................................................................................ 1-18
      1.4.2 binary ......................................................................................................... 1-18
      1.4.3 bye .............................................................................................................. 1-19
      1.4.4 cd................................................................................................................. 1-19
      1.4.5 cdup .......................................................................................................... 1-20
      1.4.6 close ......................................................................................................... 1-20
      1.4.7 debugging .............................................................................................. 1-21
      1.4.8 delete ....................................................................................................... 1-21
      1.4.9 dir ............................................................................................................. 1-22
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>disconnect</td>
<td>1-22</td>
</tr>
<tr>
<td>ftp</td>
<td>1-23</td>
</tr>
<tr>
<td>get</td>
<td>1-23</td>
</tr>
<tr>
<td>lcd</td>
<td>1-24</td>
</tr>
<tr>
<td>ls</td>
<td>1-24</td>
</tr>
<tr>
<td>mkdir</td>
<td>1-25</td>
</tr>
<tr>
<td>open</td>
<td>1-25</td>
</tr>
<tr>
<td>passive</td>
<td>1-26</td>
</tr>
<tr>
<td>put</td>
<td>1-27</td>
</tr>
<tr>
<td>pwd</td>
<td>1-27</td>
</tr>
<tr>
<td>quit</td>
<td>1-28</td>
</tr>
<tr>
<td>remotehelp</td>
<td>1-28</td>
</tr>
<tr>
<td>rmdir</td>
<td>1-29</td>
</tr>
<tr>
<td>user</td>
<td>1-29</td>
</tr>
<tr>
<td>verbose</td>
<td>1-30</td>
</tr>
<tr>
<td>TFTP Configuration Commands</td>
<td>1-30</td>
</tr>
<tr>
<td>tftp</td>
<td>1-30</td>
</tr>
<tr>
<td>tftp get</td>
<td>1-31</td>
</tr>
<tr>
<td>tftp put</td>
<td>1-31</td>
</tr>
</tbody>
</table>

Chapter 2 MAC Address Table Management Commands ......................................................... 2-1

2.1 MAC Address Table Management Commands ................................................................. 2-1
2.1.1 display mac-address aging-time ............................................................................. 2-1
2.1.2 display mac-address ............................................................................................... 2-1
2.1.3 mac-address ........................................................................................................... 2-2
2.1.4 mac-address max-mac-count .................................................................................. 2-3
2.1.5 mac-address timer .................................................................................................. 2-4

Chapter 3 Device Management Commands .............................................................................. 3-1
3.1 Device Management Commands ...................................................................................... 3-1
3.1.1 boot boot-loader ...................................................................................................... 3-1
3.1.2 boot bootrom .......................................................................................................... 3-1
3.1.3 display boot-loader .............................................................................................. 3-2
3.1.4 display cpu ........................................................................................................... 3-2
3.1.5 display device ........................................................................................................ 3-3
3.1.6 display environment .............................................................................................. 3-3
3.1.7 display fan ............................................................................................................. 3-5
3.1.8 display memory ...................................................................................................... 3-5
3.1.9 display power ........................................................................................................ 3-6
3.1.10 reboot ................................................................................................................... 3-6
3.1.11 temperature-limit ............................................................................................... 3-7

Chapter 4 System Maintenance Commands .............................................................................. 4-1
4.1 Basic System Configuration and Management Commands .............................................. 4-1
## Table of Contents

### 4.1 Clock and Time Commands
- 4.1.1 clock datetime ......................................................................................................... 4-1
- 4.1.2 clock summer-time .................................................................................................. 4-1
- 4.1.3 clock timezone ......................................................................................................... 4-3
- 4.1.4 sysname .................................................................................................................. 4-3

### 4.2 System Status and System Information Display Commands
- 4.2.1 display clock ............................................................................................................ 4-4
- 4.2.2 display current-configuration ................................................................................... 4-5
- 4.2.3 display debugging ................................................................................................... 4-9
- 4.2.4 display saved-configuration ................................................................................... 4-10
- 4.2.5 display users ......................................................................................................... 4-12
- 4.2.6 display version ....................................................................................................... 4-13

### 4.3 System Debug Commands
- 4.3.1 debugging.............................................................................................................. 4-13
- 4.3.2 display diagnostic-information ............................................................................... 4-14

### 4.4 Network Connection Test Commands
- 4.4.1 ping ........................................................................................................................ 4-15
- 4.4.2 tracert .................................................................................................................... 4-17

### 4.5 Log Commands
- 4.5.1 display channel ...................................................................................................... 4-19
- 4.5.2 display info-center ................................................................................................. 4-20
- 4.5.3 info-center channel name ...................................................................................... 4-21
- 4.5.4 info-center console channel .................................................................................. 4-21
- 4.5.5 info-center enable ................................................................................................. 4-22
- 4.5.6 info-center logbuffer ............................................................................................. 4-23
- 4.5.7 info-center loghost ............................................................................................... 4-24
- 4.5.8 info-center loghost source .................................................................................... 4-24
- 4.5.9 info-center monitor channel ................................................................................... 4-25
- 4.5.10 info-center snmp channel .................................................................................... 4-26
- 4.5.11 info-center source ............................................................................................... 4-27
- 4.5.12 info-center switch-on ........................................................................................... 4-29
- 4.5.13 info-center timestamp .......................................................................................... 4-30
- 4.5.14 info-center trapbuffer .......................................................................................... 4-30
- 4.5.15 reset logbuffer ...................................................................................................... 4-31
- 4.5.16 reset trapbuffer ................................................................................................... 4-32
- 4.5.17 terminal debugging ............................................................................................. 4-32
- 4.5.18 terminal logging .................................................................................................. 4-33
- 4.5.19 terminal monitor .................................................................................................. 4-33
- 4.5.20 terminal trapping ................................................................................................. 4-34

### 5.1 SNMP Configuration Commands
- 5.1.1 display snmp-agent community ........................................................................... 5-1
- 5.1.2 display snmp-agent ............................................................................................... 5-1
### Table of Contents

5.1.3 display snmp-agent group ................................................................. 5-2
5.1.4 display snmp-agent mib-view .......................................................... 5-3
5.1.5 display snmp-agent statistics ............................................................. 5-4
5.1.6 display snmp-agent sys-info contact ................................................ 5-5
5.1.7 display snmp-agent sys-info location ............................................... 5-6
5.1.8 display snmp-agent sys-info version ............................................... 5-6
5.1.9 display snmp-agent usm-user ........................................................... 5-7
5.1.10 snmp-agent local-engineid .............................................................. 5-8
5.1.11 snmp-agent community ................................................................. 5-8
5.1.12 snmp-agent group .......................................................................... 5-9
5.1.13 snmp-agent mib-view ...................................................................... 5-10
5.1.14 snmp-agent packet max-size .......................................................... 5-11
5.1.15 snmp-agent sys-info ........................................................................ 5-11
5.1.16 snmp-agent target-host ................................................................... 5-12
5.1.17 snmp-agent trap enable ................................................................. 5-13
5.1.18 snmp-agent trap life ....................................................................... 5-14
5.1.19 snmp-agent trap queue-size ............................................................ 5-15
5.1.20 snmp-agent trap source ................................................................. 5-16
5.1.21 snmp-agent usm-user ..................................................................... 5-16
5.1.22 undo snmp-agent ........................................................................... 5-17

### Chapter 6 RMON Configuration Commands ...................................................... 6-1

6.1 RMON Configuration Commands ............................................................ 6-1
  6.1.1 display rmon alarm ........................................................................ 6-1
  6.1.2 display rmon event ........................................................................ 6-2
  6.1.3 display rmon eventlog ..................................................................... 6-3
  6.1.4 display rmon history ....................................................................... 6-4
  6.1.5 display rmon prialarm ................................................................. 6-5
  6.1.6 display rmon statistics ................................................................. 6-7
  6.1.7 rmon alarm .................................................................................. 6-8
  6.1.8 rmon event .................................................................................. 6-9
  6.1.9 rmon history ............................................................................... 6-10
  6.1.10 rmon prialarm .......................................................................... 6-11
  6.1.11 rmon statistics .......................................................................... 6-12

### Chapter 7 NTP Configuration Commands .......................................................... 7-1

7.1 NTP Configuration Commands ............................................................... 7-1
  7.1.1 debugging ntp-service ................................................................. 7-1
  7.1.2 display ntp-service sessions ......................................................... 7-2
  7.1.3 display ntp-service status .............................................................. 7-2
  7.1.4 display ntp-service trace ............................................................... 7-4
  7.1.5 ntp-service access ....................................................................... 7-4
  7.1.6 ntp-service authentication enable ................................................. 7-5
  7.1.7 ntp-service authentication-keyid .................................................... 7-6
7.1.8 ntp-service broadcast-client ................................................................. 7-6
7.1.9 ntp-service broadcast-server ............................................................... 7-7
7.1.10 ntp-service max-dynamic-sessions .................................................. 7-8
7.1.11 ntp-service multicast-client .............................................................. 7-8
7.1.12 ntp-service multicast-server ............................................................. 7-9
7.1.13 ntp-service refclock-master ............................................................ 7-10
7.1.14 ntp-service reliable authentication-keyid ........................................ 7-11
7.1.15 ntp-service source-interface ............................................................ 7-12
7.1.16 ntp-service in-interface disable ..................................................... 7-12
7.1.17 ntp-service unicast-peer ................................................................. 7-13
7.1.18 ntp-service unicast-server ............................................................... 7-14

Chapter 8 SSH Configuration Commands .................................................. 8-1
8.1 SSH Configuration Commands ............................................................. 8-1
  8.1.1 debugging rsa .................................................................................. 8-1
  8.1.2 debugging ssh server ................................................................. 8-1
  8.1.3 display rsa local-key-pair public .................................................. 8-2
  8.1.4 display rsa peer-public-key ......................................................... 8-3
  8.1.5 display ssh server ................................................................. 8-4
  8.1.6 display ssh user-information ....................................................... 8-5
  8.1.7 peer-public-key end ................................................................. 8-5
  8.1.8 protocol inbound ......................................................................... 8-6
  8.1.9 public-key-code begin ............................................................... 8-7
  8.1.10 public-key-code end ............................................................... 8-8
  8.1.11 rsa local-key-pair create ......................................................... 8-8
  8.1.12 rsa local-key-pair destroy ......................................................... 8-9
  8.1.13 rsa peer-public-key ............................................................... 8-10
  8.1.14 ssh server authentication-retries ........................................... 8-11
  8.1.15 ssh server rekey-interval ......................................................... 8-11
  8.1.16 ssh server timeout ............................................................... 8-12
  8.1.17 ssh user assign rsa-key .......................................................... 8-12
  8.1.18 ssh user username authentication-type ................................... 8-13
Chapter 1 File System Management Commands

1.1 File System

1.1.1 cd

Syntax

cd directory

View

User view

Parameter

directory: Destination directory; By default, the directory is the working path configured by the user when the system starts.

Description

Using cd command, you can change the current user configuration path on the Ethernet Switch.

Example

# Change the current working directory of the switch to flash.
<Quidway>cd flash:
<Quidway>pwd
flash:

1.1.2 copy

Syntax

copy fileurl-source fileurl-dest

View

User view

Parameter

fileurl-source: Source file name.
fileurl-dest: Destination file name.
Description

Using `copy` command, you can 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.
<Quidway> dir
Directory of *
 0  -rw-    595  Jul 12 2001 19:41:50   test.txt
16125952 bytes total (13975552 bytes free)

# Copy the file test.txt and saves it as test.bak.
<Quidway> copy test.txt test.bak
Copy flash:/test/test.txt to flash:/test/test.bak ?[confirm]:y
% Copied file flash:/test/test.txt flash:/test/test.bak

# Display current directory information.
<Quidway> dir
Directory of *
 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)
```

1.1.3 delete

Syntax

`delete [ /unreserved ] file-url`

View

User view

Parameter

`file-url`: path and name of the file you want to delete.

Description

Using `delete` command, you can delete a specified file from the storage device of the Ethernet 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.
Note that, 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
<Quidway> delete flash:/test/test.txt
Delete flash:/test/test.txt?[Y/N]:

1.1.4 dir

Syntax

dir [/all] [ file-url ]

View

User view

Parameter

/all: Display all the files (including the deleted ones).

file-url: File or directory name to be displayed. The file-url parameter supports "*" matching. For example, using dir *.{txt will display all the files with the extension.txt in the current directory.; By default, display the file information in current path.

Description

Using dir command, you can view the information about the specified file or directory in storage device of Ethernet Switch.

Example

# Display the information about the file flash:/test/test.txt
<Quidway> dir flash:/test/test.txt
Directory of flash:/test/
-rwxrwxrwx 1 noone nogroup 971 Sep 20 2003 14:28:52 test.txt
7932928 bytes total (4966400 bytes free)

# Display information of directory flash:/test/
<Quidway> dir flash:/test/
Directory of flash:/test/
-rwxrwxrwx 1 noone nogroup 971 Sep 20 2003 14:28:52 test.txt
7932928 bytes total (4966400 bytes free)

# Display all files with the names starting with "t" in the directory flash:/test/
<Quidway> dir flash:/test/t*
Directory of flash:/test/
-rwxrwxrwx 1 noone nogroup 971 Sep 20 2003 14:28:52 test.txt
# Display information about all the files (including the deleted files) in the directory flash:/test/

```
<Quidway> dir /all flash:/test/
Directory of flash:/test/
-rwxrwxrwx 1 noone nogroup 971 Sep 20 2003 14:28:52 test.txt
```

# Display information of all the files (including the deleted files) with the names starting with "t" in flash:/test/

```
<Quidway> dir /all flash:/test/t*
Directory of flash:/test/t*
-rwxrwxrwx 1 noone nogroup 971 Sep 20 2003 14:32:49 [text.txt]
```

---

**Note:**

In the output information of `dir/all` command, as a hint, the name of each deleted file kept in the recycle bin is in a square bracket.

---

### 1.1.5 file prompt

**Syntax**

```
file prompt \{ alert | quiet \}
```

**View**

System view

**Parameter**

- **alert:** Perform interactive confirmation on dangerous file operations; The default value is **alert**, which configures to perform interactive confirmation on dangerous file operations.
- **quiet:** Do not prompt for the file operations.

**Description**

Using `file prompt` command, you can modify prompt modes of the file operation on the Ethernet switch.

If the prompt mode is set as **quiet**, that is, no prompt for file operations, some non-recoverable operations may lead to system damage.
Example

# Configure the prompt mode of file operation as quiet.
[Quidway] file prompt quiet

1.1.6 format

Syntax

format filesystem

View

User view

Parameter

filesystem: Device name.

Description

Using format command, you can format the storage device.
Format operation will cause non-recoverable loss of all the files on the device. Specially, configuration files will be lost after formatting the flash memory.

Example

# Format flash:
<Quidway> format flash:
All data on Flash will be lost, proceed with format? [Y/N] y
% Now begin to format flash, please wait for a while...
Format winc: completed

1.1.7 mkdir

Syntax

mkdir directory

View

User view

Parameter

directory: Directory name.

Description

Using mkdir command, you can create directory in the specified directory on the storage device.
The directory to be created cannot have the same name as that of other directory or file in the specified directory.

Example

```
# Create the directory dd.
<Quidway> mkdir dd
% Created dir dd
```

1.1.8 more

Syntax

```
more file-url
```

View

User view

Parameter

`file-url`: File name.

Description

Using `more` command, you can view content of specified file. At present, file system can display files in the text format.

Example

```
# Display contents of file test.txt.
<Quidway> 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.
```

1.1.9 move

Syntax

```
move fileurl-source fileurl-dest
```

View

User view
Parameter

fileurl-source: Source file name.

fileurl-dest: Destination file name.

Description

Using move command, you can move files.

When the destination filename is the same as that of an existing file, the system will ask whether to overwrite it.

Example

# Display the current directory information.

<Quidway> dir
Directory of flash:/
  drwxrwxrwx 1 noone nogroup - Jun 22 2002 02:19:16 shit
  -rwxrwxrwx 1 noone nogroup 971 Jun 30 2003 11:45:19 vrpcfg.txt
  -rwxrwxrwx 1 noone nogroup 4 Aug 27 2003 16:56:56 snmpboots
  -rwxrwxrwx 1 noone nogroup 2957562 Sep 20 2003 10:49:57 QX-S5516-VRP31-0-0030.app
  drwxrwxrwx 1 noone nogroup - Sep 20 2003 14:27:58 test
<Quidway> dir flash:/test/
Directory of flash:/test/
  drwxrwxrwx 1 noone nogroup - Sep 20 2003 14:36:11 dd
  -rwxrwxrwx 1 noone nogroup 971 Sep 20 2003 14:40:05 sample.txt
7932928 bytes total (4963328 bytes free)

# Move flash:/test/sample.txt to flash:/sample.txt.

<Quidway> move flash:/test/sample.txt flash:/sample.txt
Move flash:/test/sample.txt to flash:/sample.txt ?[Y/N]:y
% Moved file flash:/test/sample.txt to flash:/sample.txt

# Display the directory after moving a file.

<Quidway> dir
Directory of flash:/
  drwxrwxrwx 1 noone nogroup - Jun 22 2002 02:19:16 shit
  -rwxrwxrwx 1 noone nogroup 971 Jun 30 2003 11:45:19 vrpcfg.txt
  -rwxrwxrwx 1 noone nogroup 4 Aug 27 2003 16:56:56 snmpboots
  -rwxrwxrwx 1 noone nogroup 2957562 Sep 20 2003 10:49:57 QX-S5516-VRP31-0-0030.app
  drwxrwxrwx 1 noone nogroup - Sep 20 2003 14:27:58 test
  -rwxrwxrwx 1 noone nogroup 971 Sep 20 2003 14:41:44 sample.txt
7932928 bytes total (4963328 bytes free)
<Quidway> dir flash:/test/
Directory of flash:/test/
drwxrwxrwx 1 noone nogroup - Sep 20 2003 14:36:11 dd
7932928 bytes total (4963328 bytes free)

1.1.10  pwd

Syntax
pwd

View
User view

Parameter
none

Description
Using pwd command, you can view the current path.
Error may occur without setting the current path.

Example
# Display the current path.
<Quidway> pwd
flash:

1.1.11  rename

Syntax
rename fileurl-source fileurl-dest

View
User view

Parameter
fileurl-source: Source file name.
fileurl-dest: Destination file name.

Description
Using rename command, you can rename a file.
If the destination file name is the same as an existing directory name, operation fails. If the destination file name is the same as an existing file name, prompt whether to overwrite.
Example

# Display the current directory information.

<Quidway> dir
Directory of flash:/
drwxrwxrwx 1 noone nogroup - Jun 22 2002 02:19:16 shit
-rwxrwxrwx 1 noone nogroup 971 Jun 30 2003 11:45:19 vrpcfg.txt
-rwxrwxrwx 1 noone nogroup 4 Aug 27 2003 16:56:56 snmpboots
-rwxrwxrwx 1 noone nogroup 2957562 Sep 20 2003 10:49:57 QX-S5516-VRP31 0-0030.app
drwxrwxrwx 1 noone nogroup - Sep 20 2003 14:27:58 test
-rwxrwxrwx 1 noone nogroup 971 Sep 20 2003 14:41:44 sample.txt
7932928 bytes total (4963328 bytes free)

# Rename the file sample.txt with sample.bak.

<Quidway> rename sample.txt sample.bak
Rename flash:/sample.txt to flash:/sample.bak ?[Y/N]:y
% Renamed file flash:/sample.txt to flash:/sample.bak

# Display the directory after renaming sample.txt with sample.bak.

<Quidway>dir
Directory of flash:/
drwxrwxrwx 1 noone nogroup - Jun 22 2002 02:19:16 shit
-rwxrwxrwx 1 noone nogroup 971 Jun 30 2003 11:45:19 vrpcfg.txt
-rwxrwxrwx 1 noone nogroup 4 Aug 27 2003 16:56:56 snmpboots
-rwxrwxrwx 1 noone nogroup 2957562 Sep 20 2003 10:49:57 QX-S5516-VRP31 0-0030.app
drwxrwxrwx 1 noone nogroup - Sep 20 2003 14:27:58 test
-rwxrwxrwx 1 noone nogroup 971 Sep 20 2003 14:44:54 sample.bak
7932928 bytes total (4962304 bytes free)

1.1.12  reset recycle-bin

Syntax

reset recycle-bin file-url

View

User view

Parameter

file-url: Name of the file to be deleted.
Description

Using **reset recycle-bin** command, you can permanently delete files from the recycle bin.

The **delete** command only puts the file into the recycle bin, but **reset recycle-bin** command will delete this file permanently.

Example

```
# Delete the file from the recycle bin.
<Quidway> reset recycle-bin flash:/plh_logic.out
Clear flash:/plh_logic.out? [Y/N]:
```

1.1.13 rmdir

**Syntax**

```
rmdir directory
```

**View**

User view

**Parameter**

*directory*: Directory name.

**Description**

Using **rmdir** command, you can cancel a directory.

The directory to be deleted must be empty.

**Example**

```
# Delete the directory huawei.
<Quidway> rmdir huawei
Rmdir huawei?[Y/N]:y
% Removed directory huawei
```

1.1.14 undelete

**Syntax**

```
undelete file-url
```

**View**

User view
Parameter

file-url: Name of the file to be recovered.

Description

Using undelete command, you can recover 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, prompt whether to overwrite.

Example

# Display the information of all the files (including the deleted ones) in the current directory.
<Quidway> dir /all
Directory of flash:/
   drwxrwrwx  1 noone  nogroup   -  Jun 22 2002 02:19:16  shit
   -rwxrwxrwx  1 noone  nogroup       971  Jun 30 2003 11:45:19  vrpcfg.txt
   -rwxrwxrwx  1 noone  nogroup        4 Aug 27 2003 16:56:56  snmpboots
   -rwxrwxrwx  1 noone  nogroup 2957562 Sep 20 2003 10:49:57  QX-S5516-VRP31 0-0030.app
   drwxrwxrwx  1 noone  nogroup   -  Sep 20 2003 14:27:58  test
   -rwxrwxrwx  1 noone  nogroup       971 Sep 20 2003 14:53:32  [sample.bak]
7932928 bytes total (4962304 bytes free)

# Recover the deleted file sample.bak.
<Quidway> undelete sample.bak
Undelete flash:/sample.bak ?[Y/N]:y
% Undeleted file flash:/sample.bak

# Display the information of all the files (including the deleted ones) in the current directory.
<Quidway> dir /all
Directory of flash:/
    drwxrwxrwx  1 noone  nogroup   -  Jun 22 2002 02:19:16  shit
   -rwxrwxrwx  1 noone  nogroup       971 Jun 30 2003 11:45:19  vrpcfg.txt
   -rwxrwxrwx  1 noone  nogroup        4 Aug 27 2003 16:56:56  snmpboots
   -rwxrwxrwx  1 noone  nogroup 2957562 Sep 20 2003 10:49:57  QX-S5516-VRP31 0-0030.app
   drwxrwxrwx  1 noone  nogroup   -  Sep 20 2003 14:27:58  test
   -rwxrwxrwx  1 noone  nogroup       971 Sep 20 2003 14:54:16  sample.bak
7932928 bytes total (4962304 bytes free)
1.2 Configuration File Management Commands

1.2.1 reset saved-configuration

Syntax

reset saved-configuration

View

User view

Parameter

none

Description

Using reset saved-configuration command, you can erase configuration files from the flash memory of the Ethernet Switch.

Perform this command with cautious. It is suggested to consult technical support personnel first.

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.
- If a used Ethernet Switch is applied to the new circumstance and the original configuration files cannot meet the new requirements, the Ethernet Switch should be configured again. Erase the original configuration files for reconfiguration.

If the configuration files do not exist in the flash memory when Ethernet Switch is electrified and initialized, it will enter setup switch view automatically.

For the related commands, see save, display current-configuration, display saved-configuration.

Example

# Erase the configuration files from the flash memory of Ethernet Switch.
<Quidway> reset saved-configuration
This will delete the configuration in the flash memory.
The switch configurations will be erased to reconfigure.
Are you sure?[Y/N]
1.2.2  save

Syntax

save

View

User view

Parameter

none

Description

Using save command, you can save the current configuration files to Flash memory. After finishing a group of configurations and achieving corresponding functions, user should remember to get the current configuration files stored in the flash memory. For the related commands, see reset saved-configuration, display current-configuration, display saved-configuration.

Example

# Get the current configuration files stored in the flash memory.
<Quidway> save
This will save the configuration in the flash memory.
The switch configurations will be written to flash.
Are you sure?[Y/N]
Now saving current configuration to flash memory.
Please wait for a while...
Save current configuration to flash memory successfully.

1.3  FTP Server Configuration Commands

1.3.1  display ftp-server

Syntax

display ftp-server

View

Any view

Parameter

none
Description

Using **display ftp-server** command, you can view 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.
<Quidway> display ftp-server
    FTP server is running
    Max user number       5
    User count            0
    Timeout value(in minute)       30
```

### 1.3.2 display ftp-user

**Syntax**

```
display ftp-user
```

**View**

Any view

**Parameter**

none

**Description**

Using **display ftp-user** command, you can view 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.
<Quidway> display ftp-user
% No ftp user
```

### 1.3.3 ftp server

**Syntax**

```
ftp server enable
undo ftp server
```

Huawei Technologies Proprietary
View

System view

Parameter

enable: Start FTP Server.

Description

Using `ftp server` command, you can start FTP Server and enable FTP user logon. Using `undo ftp server` command, you can 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 Ethernet Switch from being attacked by some unknown user.

Example

# Shut down FTP Server.
[Quidway] undo ftp server

1.3.4 ftp timeout

Syntax

`ftp timeout minute`
`undo ftp timeout`

View

System view

Parameter

`minute`: Connection timeouts (measured in minutes), ranging from 1 to 35791; By default, the connection timeout time is 30 minutes.

Description

Using `ftp timeout` command, you can configure connection timeout interval. Using `undo ftp timeout` command, you can 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 be failed and disconnect to the client.
Example

# Set the connection timeout to 36 minutes.
[Quidway] ftp timeout 36

1.3.5 local-user

Syntax

local-user user-name

undo local-user { user-name | all [ service-type { telnet | ftp | lan-access } ] }

View

System view

Parameter

user-name: Specifies a local username with a character string not exceeding 32 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 24 characters.

service-type: Specifies the service type. telnet means that: the specified user type is telnet. ftp means that: the specified user type is ftp. lan-access means that the specified user type is lan-access which mainly refers to Ethernet accessing users, 802.1x supplicants for example.

all: All the users.

Description

Using local-user command, you can configure a local user and enter the local user view. Using undo local-user command, you can cancel a specified local user.

By default, no local user.

For the related commands, see display local-user, server-type.

Example

# Add a local user named huawei1.
[Quidway] local-user huawei1
[Quidway-user-huawei1]

1.3.6 password

Syntax

password { simple | cipher } password

undo password

Huawei Technologies Proprietary
View

Local user view

Parameter

**simple**: Specifies to display passwords in simple text.

**cipher**: Specifies to display passwords in cipher text.

**password**: Defines a password, which is a character string of up to 16 characters if it is in simple text and of up to 24 characters if it is in cipher text.

Description

Using **password** command, you can configure a password display mode for local users. Using **undo password** command, you can cancel the specified password display mode.

If **local-user password-display-mode cipher-force** has been adopted, the user efforts of using the **password** command to set the password display mode to simple text (**simple**) will render useless.

For the related command, see **display local-user**.

Example

```
# Set the user huawei1 to display the password in simple text, given the password is 20030422.
[Quidway-user-huawei1] password simple 20030422
```

1.3.7 service-type

Syntax

```
service-type \{ telnet \[ level level \] | ftp \[ ftp-directory directory \] | lan-access \}
undo service-type \{ telnet \[ level \] | ftp \[ ftp-directory \] | lan-access \}
```

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 3.

**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.

**Description**

Using **service-type** command, you can configure a service type for a particular user. Using **undo service-type** command, you can cancel the specified service type for the user.

**Example**

```
# Set to provide the lan-access service for the user huawei1.
[Quidway-user-huawei1] service-type lan-access
```

### 1.4 FTP Client Commands

#### 1.4.1 ascii

**Syntax**

```
ascii
```

**View**

FTP Client view

**Parameter**

```
none
```

**Description**

Using **ascii** command, you can 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.
[ftp] ascii
200 Type set to A.
```

#### 1.4.2 binary

**Syntax**

```
binary
```

**Example**

```
# Configure to transmit data in the ASCII mode.
[ftp] ascii
200 Type set to A.
```
View

FTP Client view

Parameter

none

Description

Using **binary** command, you can configure file transmission type as binary mode.

Example

# Configure to transmit data in the binary mode.

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

1.4.3 **bye**

Syntax

```
bye
```

View

FTP Client view

Parameter

none

Description

Using **bye** command, you can 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.

```
[ftp] bye
```

1.4.4 **cd**

Syntax

```
cd pathname
```
View

FTP Client view

Parameter

**pathname**: Path name.

Description

Using `cd` command, you can 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
[ftp] cd flash:/temp
```

1.4.5 cdup

Syntax

cdup

View

FTP Client view

Parameter

none

Description

Using `cdup` command, you can 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.
[ftp] cdup
```

1.4.6 close

Syntax

close
**Close**

**Syntax**

close

**View**

FTP Client view

**Parameter**

none

**Description**

Using close command, user can disconnect FTP client side from FTP server side without exiting FTP client side view. That is to say, you can 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 stays in FTP Client view.

```
[ftp] close
```

**1.4.7 debugging**

**Syntax**

diagnostics

**View**

FTP Client view

**Parameter**

none

**Description**

Using debugging command, you can enable the system debugging functions.

**Example**

# Enable the system debugging functions.

```
[ftp] debugging
Debug is on.
```

**1.4.8 delete**

**Syntax**

delete remotefile

**View**

FTP Client view
Parameter

remotefile: File name.

Description

Using **delete** command, you can cancel the specified file.
This command is used to delete a file.

Example

```
# Delete the file temp.c
[ftp] delete temp.c
```

### 1.4.9 dir

**Syntax**

```
dir [ filename ] [ localfile ]
```

**View**

FTP Client view

**Parameter**

- **filename**: File name to be queried.
- **localfile**: Saved local file name.

**Description**

Using **dir** command, you can 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 saves the results in the file temp1.
[ftp] dir temp.c temp1
```

### 1.4.10 disconnect

**Syntax**

```
disconnect
```

**View**

FTP Client view
Parameter

none

Description

Using `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 stays in FTP Client view.
[ftp] disconnect

1.4.11 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

Using `ftp` command, you can 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
<Quidway> ftp 1.1.1.1

1.4.12 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

Using the `get` command, you can 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
[ftp] get temp1.c temp.c
```

1.4.13 lcd

Syntax

```
lcd
```

View

FTP Client view

Parameter

- none

Description

Using the `lcd` command, you can view local working path of FTP Client.

Example

```
# Show local working path.
[ftp] lcd
% Local directory now flash:/temp
```

1.4.14 ls

Syntax

```
ls [ remotefile ] [ localfile ]
```

View

FTP Client view
Parameter

- remotefile: Remote file to be queried.
- localfile: Saved local file name.

Description

Using `ls` command, you can query a specified file.
If no parameter is specified, all the files will be shown.

Example

```
# Query file temp.c
[ftp] ls temp.c
```

1.4.15 mkdir

Syntax

`mkdir pathname`

View

FTP Client view

Parameter

- `pathname`: Directory name.

Description

Using `mkdir` command, you can create a directory on the remote FTP Server.
User can perform this operation as long as the remote FTP server has authorized.

Example

```
# Create the directory flash:/lanswitch on the remote FTP Server.
[ftp] mkdir flash:/lanswitch
```

1.4.16 open

Syntax

```
open [ ip-address [ port ]]
```

View

FTP Client view
Parameter

`ip-address`: The host name (a string with a length of 1 to 20 characters) or the IP address of the remote FTP Server.

`port`: Port number of remote FTP Server, ranging from 0 to 65535. By default, it is 21.

Description

Using **open** command, you can establish control connection with the remote FTP Server in the FTP Client view.

Related command: **close**.

Example

```
# Establish control connection with the FTP Server, which IP address is 1.1.1.1.
[ftp] open 1.1.1.1
Trying ...
Press CTRL+K to abort
Connected.
220- WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(none): abc
331 Give me your password, please
Password:
230 Logged in successfully
```

1.4.17 passive

Syntax

```
passive
undo passive
```

View

FTP Client view

Parameter

```
none
```

Description

Using **passive** command, you can configure the data transmission mode as passive mode. Using **undo passive** command, you can configure the data transmission mode as active mode.

By default, the data transmission mode is passive mode.
Example

# Set the data transmission to passive mode.
[ftp] passive

1.4.18 put

Syntax

put localfile [ remotefile ]

View

FTP Client view

Parameter

localfile: Local file name.
remotefile: File name on the remote FTP Server.

Description

Using put command, you can 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.
[ftp] put temp.c temp1.c

1.4.19 pwd

Syntax

pwd

View

FTP Client view

Parameter

none

Description

Using pwd command, you can view the current directory on the remote FTP Server.
Example

# Show the current directory on the remote FTP Server.
[ftp] pwd
"flash:/temp" is current directory.

1.4.20 quit

Syntax

quit

View

FTP Client view

Parameter

none

Description

Using quit command, you can terminate the connection with the remote FTP Server and return to user view.

Example

# Terminate connection with the remote FTP Server and returns to user view.
[ftp] quit
<Quidway>

1.4.21 remotehelp

Syntax

remotehelp [ protocol-command ]

View

FTP Client view

Parameter

protocol-command: FTP protocol command.

Description

Using remotehelp command, you can view help information about the FTP protocol command.
Example

# Show the syntax of the protocol command user.
[ftp] remotehelp user
214 Syntax: USER <sp> <username>

1.4.22 rmdir

Syntax

rmdir pathname

View

FTP Client view

Parameter

pathname: Directory name of remote FTP Server.

Description

Using rmdir command, you can cancel the specified directory from FTP Server.

Example

# Delete the directory flash:/temp1 from FTP Server.
[ftp] rmdir flash:/temp1

1.4.23 user

Syntax

user username [password]

View

FTP Client view

Parameter

username: Logon username.
password: Logon password.

Description

Using user command, you can register an FTP user.

Example

# Log in the FTP Server with username tom and password bjhw.
[ftp] user tom bjhw
1.4.24 verbose

Syntax

verbose
undo verbose

View

FTP Client view

Parameter

none

Description

Using verbose command, you can enable verbose. Using undo verbose command, you can disable verbose.
By default, verbose is enabled.

Example

# Enable verbose.
[ftp]verbose

1.5 TFTP Configuration Commands

1.5.1 tftp

Syntax

tftp { ascii | binary }

View

System view

Parameter

ascii: Text format.

binary: Binary format; By default, the transmission mode is binary.

Description

Using tftp command, you can configure the transmission mode of the TFTP files.
TFTP transmits files in two modes, binary mode for program files and ASCII mode for text files. You can perform this command to configure the file transmission mode. By
default, TFTP transmits files in binary mode. Before resetting the mode and restarting the switch, the set mode will not change.

For the related commands, see **tftp get, tftp put**.

**Example**

```
# Transmit the files in text format.
[Quidway] tftp ascii
```

### 1.5.2 tftp get

**Syntax**

```
tftp get //A.A.A.A/xxx.yyy mmm.nnn
```

**View**

System view

**Parameter**

- `//A.A.A.A/xxx.yyy`: Information about the file to be downloaded from the TFTP server.
- `A.A.A.A`: IP address of the TFTP server.
- `mmm.nnn`: Specify the filename saved as after downloaded to the switch, which can be different from `xxx.yyy`.

**Description**

Using **tftp get** command, you can download a file `xxx.yyy` from the specified directory of the TFTP server (at `A.A.A.A`) and saving it as `mmm.nnn` on the switch.

For the related commands, see **tftp, 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.
[Quidway] tftp binary
[Quidway] tftp get //1.1.3.214/ LANSwitch.app vxWorks.app
```

### 1.5.3 tftp put

**Syntax**

```
tftp put mmm.nnn //A.A.A.A/xxx.yyy
```

**View**

System view
Parameter

\textit{mmm.nnn}: The file to be uploaded.

\textit{//A.A.A.A/xxx.yyy}: IP address of the TFTP server and the filename to be saved as.

Description

Using \texttt{tftp put} command, you can upload a file from the switch to the specified directory on the TFTP server (at \texttt{A.A.A.A}) and saving it as \textit{mmm.nnn}.

For the related commands, see \texttt{tftp, tftp get}.

Example

\begin{verbatim}
# Upload the vrpcfg.txt to the TFTP server at 1.1.3.214 and save it as Temp.txt.
[Quidway] tftp ascii
[Quidway] tftp put vrpcfg.txt //1.1.3.214/temp.txt
\end{verbatim}
Chapter 2 MAC Address Table Management Commands

2.1 MAC Address Table Management Commands

2.1.1 display mac-address aging-time

Syntax

display mac-address aging-time

View

Any view

Parameter

none

Description

Using display mac-address aging-time command, you can view 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.

Example

# Display the aging time of the dynamic entry in the MAC address table.
[Quidway] 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.

2.1.2 display mac-address

Syntax

display mac-address [ mac-addr [ vlan vlan-id ] | [ static | dynamic ] [ interface { interface-name | interface-type interface-num } ] [ vlan vlan-id ] [ count ] ]

View

Any view
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.
- **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 sum number of MAC addresses in the MAC address table if user choice this parameter when using this command.

Description

Using `display mac-address` command, you can view 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
[Quidway] display mac-address 00e0-fc01-0101

MAC ADDR  VL AN ID  STATE   PORT INDEX   AGING TIME
00e0-fc01-0101 1  Learned   Ethernet0/1  AGING
```

2.1.3 mac-address

Syntax

```
mac-address { static | dynamic } mac-addr interface { interface-name | interface-type interface-num } vlan vlan-id
undo mac-address [ static | dynamic ] [ [ mac-addr ] 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.

**mac-addr**: Specify the MAC address.

**interface-type**: interface type;

**interface-num**: interface number;

**interface-name**: interface name;

**vlan-id**: Specify the VLAN ID.

Description

Using **mac-address** command, you can add/modify the MAC address table entry. Using **undo mac-address** command, you can cancel MAC address table entry.

If the input address has been existed 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.

Because the address table is shared in the VLAN domain, you need specify the VLAN of the multicast address and the port of the unicast address, when adding entries to the address table.

For the related commands, see **display mac-address**.

Example

```
# Configure the port number corresponding to the MAC address 00e0-fc01-0101 as Ethernet0/1 in the address table, and sets this entry as static entry.
[Quidway] mac-address static 00e0-fc01-0101 interface ethernet 0/1 vlan 2
```

2.1.4 **mac-address max-mac-count**

Syntax

```
mac-address max-mac-count count
undo mac-address max-mac-count
```

View

Ethernet port view
Parameter

$count$: Specify the amount limit to the MAC addresses to be learned. 0 indicates that no address can be learned via the port.

Description

Using `mac-address max-mac-count` command, you can set a limit to the MAC addresses to be learned by the Ethernet port. Using `undo mac-address max-mac-count` command, you can cancel the limit.

By default, there is no limit to the MAC addresses learned via the Ethernet port.

The port will stop learning MAC address when the amount reaches the limit specified by the `count` parameter.

For the related commands, see `mac-address, mac-address timer`.

Example

```
# Configure Ethernet0/3 to learn at most 600 addresses.
[Quidway-Ethernet0/3] mac-address max-mac-count 600

# Configure no limit to the amount of addresses learned via Ethernet0/3.
[Quidway-Ethernet0/3] undo mac-address max-mac-count
```

2.1.5 `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

Using `mac-address timer` command, you can configure the aging time of the Layer-2 dynamic address table entry. Using `undo mac-address timer` command, you can restore the default value.
Too long or too short aging time set by subscribers will cause the problem that the Ethernet switch broadcasts a great mount of data packets without MAC addresses, which will affect the switch operation performance.

If aging time is set too long, the Ethernet switch will store a great number of 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 Ethernet switch may delete valid MAC address table.

**Example**

```
# Configure the entry aging time of Layer-2 dynamic address table to be 500 seconds.
[Quidway] mac-address timer aging 500
```
Chapter 3 Device Management Commands

3.1 Device Management Commands

3.1.1 boot boot-loader

Syntax

```
boot boot-loader file-url
```

View

User view

Parameter

- `file-url`: Path and name of APP file.

Description

Using `boot boot-loader` command, you can configure the app file used for boot of the next time.

Example

```
# Specify the APP application used for boot of next time.
<Quidway> boot boot-loader PLATV100R002B09D002.APP
The specified file will be booted next time!
<Quidway>
```

3.1.2 boot bootrom

Syntax

```
boot bootrom file-url
```

View

User view

Parameter

- `file-url`: File path and file name of Bootrom.

Description

Using `boot bootrom` command, you can upgrade bootrom.
Example

# Upgrade bootrom.

<Quidway> boot bootrom PLATV100R002B09D002.btm

3.1.3 display boot-loader

Syntax

display boot-loader

View

Any view

Parameter

none

Description

Using display boot-loader command, you can view APP file used next time.

Example

# View APP file used next time.

<Quidway> display boot-loader

The app to boot at the next time is: PLATV100R002B09D002.APP

3.1.4 display cpu

Syntax

display cpu

View

Any view

Parameter

None

Description

Using display cpu command, you can display CPU occupancy.

Example

# Display CPU occupancy.

<Quidway> display cpu

CPU busy status:
Table 3-1 Display information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU busy status.</td>
<td>The busy status of switch</td>
</tr>
<tr>
<td>18% in last 5 seconds</td>
<td>The CPU occupancy rate is 18% at last 5 seconds</td>
</tr>
<tr>
<td>19% in last 1 minute</td>
<td>The CPU occupancy rate is 19% at last 1 minute</td>
</tr>
<tr>
<td>19% in last 5 minutes</td>
<td>The CPU occupancy rate is 19% at last 5 minutes</td>
</tr>
</tbody>
</table>

3.1.5 display device

Syntax

display device

View

Any view

Parameter

none

Description

Using display device command, you can view module type and working status information of each card (including main card and daughter-card).

Perform 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, BOOTROM software version number, application version number, address learning mode, interface card type and interface card type description, etc.

Example

# Show the card information.
<Quidway> display device

SlotNo SubSNo PortNum PCBVer FPGAVer CPLDVer BootRomVer AddrLM Type
0 0 24 REV.0 001 002 360 IVL MAIN

The following table describes the displaying information.
Table 3-2 Output description of the display device command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SlotNo</td>
<td>Physical card number</td>
</tr>
<tr>
<td>SubSNo</td>
<td>Sub physical card number (namely stack card number)</td>
</tr>
<tr>
<td>PortNum</td>
<td>Number of ports</td>
</tr>
<tr>
<td>PCBVer</td>
<td>PCB version number</td>
</tr>
<tr>
<td>FPGAVer</td>
<td>FPGA version number</td>
</tr>
<tr>
<td>CPLDVer</td>
<td>Hardware version number</td>
</tr>
<tr>
<td>BootRomVer</td>
<td>BootROM software version number</td>
</tr>
<tr>
<td>AddrLM</td>
<td>Address learning mode</td>
</tr>
<tr>
<td>Type</td>
<td>Interface card type</td>
</tr>
</tbody>
</table>

3.1.6 display environment

Syntax

display environment

View

Any view

Parameter

none

Description

Using **display environment** command, you can view environment information.

Example

# Display the environment information.

<Quidway> display environment

System temperature information (degree centigrade):

<table>
<thead>
<tr>
<th>Board</th>
<th>Temperature</th>
<th>Lower limit</th>
<th>Upper limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>46</td>
<td>20</td>
<td>80</td>
</tr>
<tr>
<td>6</td>
<td>42</td>
<td>10</td>
<td>80</td>
</tr>
</tbody>
</table>
3.1.7 display fan

Syntax

display fan [ fan-id ]

View

Any view

Parameter

fan-id: the fan ID.

Description

Using display fan command, you can view the working state of the built-in fans. User can Perform this command to see if they work normally.

Example

# Display the working state of the fans.
<Quidway> display fan
Fan 1 State: Normal
Fan 2 State: Normal
Fan 3 State: Normal
Fan 4 State: Normal

The above information indicates that all of the four fans work normally.

3.1.8 display memory

Syntax

display memory [ slot slot-number ]

View

Any view

Parameter

slot-number: Specify slot number

Description

Using display memory command, you can display memory situation.

Example

# Display memory situation.
<Quidway> display memory
System Total Memory(bytes): 32491008
Total Used Memory(bytes): 13181348
Used Rate: 40%

Table 3-3 Display information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Total Memory(bytes)</td>
<td>The Total Memory of switch, unit in byte</td>
</tr>
<tr>
<td>Total Used Memory(bytes)</td>
<td>The Total used Memory of switch, unit in byte</td>
</tr>
<tr>
<td>Used Rate</td>
<td>The memory used rate</td>
</tr>
</tbody>
</table>

3.1.9 display power

Syntax

display power [ powe-ID ]

View

Any view

Parameter

powe-ID: Power ID.

Description

Using display power command, you can view the working state of the built-in power supply.

Example

# Show power state.
<Quidway> display power 1
power 1 State: Normal

3.1.10 reboot

syntax

reboot

View

User view
Parameter

none.

Description

Using `reboot` command, you can reset the Ethernet Switch when failure occurs.

Example

```
# Reboots the Switch.
<Quidway> reboot
```

### 3.1.11 temperature-limit

Syntax

```
temperature-limit slot down-value up-value
undo temperature-limit slot
```

View

User view, system view

Parameter

- **slot**: Physical card number.
- **down-value**: Lower temperature limit.
- **up-value**: Upper temperature limit.

Description

Using `temperature-limit` command, you can configure temperature limit. Using `undo temperature-limit` command, you can restore temperature limit to default value.

Example

```
# Set the lower and upper temperature limit of card 0.
<Quidway> temperature-limit 0 10 75
Success temperature limit set
```
Chapter 4  System Maintenance Commands

4.1  Basic System Configuration and Management Commands

4.1.1  clock datetime

Syntax

clock datetime  \text{HH:MM:SS\ YYYY/MM/DD}

View

User view

Parameter

\text{HH:MM:SS}: \text{Current clock. HH ranges from 0 to 23. MM and SS range from 0 to 59.}

\text{YYYY/MM/DD}: \text{Specify the current year, month and date. YYYY ranges from 1993 to 2035. MM ranges from 1 to 12 and DD ranges from 1 to 31.}

Description

Using \text{clock datetime} command, you can configure the current date and clock of Ethernet Switch.

By default, the date and clock of Ethernet Switch is set as 0:0:0, 2000/1/1.

The current date and clock of Ethernet Switch must be set in the circumstance that absolute time is strictly required.

For the related commands, see \text{display clock}.

Example

# Set the current date of Ethernet Switch to 0:0:0, 2001/01/1.
<Quidway> clock datetime 0:0:0 2001/01/01

4.1.2  clock summer-time

Syntax

clock summer-time  \text{zone_name \{one-off | repeating\} \ start-time \ start-date \ end-time \ end-date \ offset-time }

undo clock summer-time

Huawei Technologies Proprietary
View

User view

Parameter

*zone_name*: Name of the summer time, which is a character with the length ranging 1 to 32.

*one-off*: Only set the summer time of a certain year.

*repeating*: Set the summer time of every year starting from a certain year.

*start-time*: Set start time of the summer time, input like *HH:MM:SS* (hour/minute/second).

*start-date*: Set start time of the summer time, input like *YYYY/MM/DD* (year/month/day).

*end-time*: Set end time of the summer time, input like *HH:MM:SS* (hour/minute/second).

*end-date*: Set end time of the summer time, input like *YYYY/MM/DD* (year/month/day).

*offset-time*: Set offset time of the summer time, input like *HH:MM:SS* (hour/minute/second).

Description

Using *clock summer-time* command, you can set the name, starting and ending time of the summer time. Using *undo clock summer-time* command, you can remove the configuration of the summer time.

After the configuration takes effect, the *display clock* command can be used to check it. Besides, the time of the log or debug information uses the local time after the adjustment of the time zone and summer time.

For the related command, see *clock timezone*.

Example

# Set the summer time for z2 that starts at 06:00:00 on 08/06/2002 and ends at 06:00:00 on 01/09/2002 with the time adding 1 hour.
<Quidway> clock summer-time z2 one-off 06:00:00 2002/06/08 06:00:00 2002/09/01 01:00:00

# Set the summer time for z2 that starts at 06:00:00 on 08/06 and ends at 06:00:00 on 01/09 in each year from 2002 on with the time adding 1 hour.
<Quidway> clock summer-time z2 repeating 06:00:00 2002/06/08 06:00:00 2002/09/01 01:00:00
4.1.3 clock timezone

Syntax

```
clock timezone zone_name { add | minus } HH:MM:SS
```

```
undo clock timezone
```

View

User view

Parameter

```
zone_name: Name of the time zone, which is a character with the length ranging 1 to 32.
add: The time is adding compared with the UTC.
minus: The time is minus compared with the UTC.
```

Description

Using `clock timezone` command, you can set the information of the local time zone. Using `undo clock timezone` command, you can restore to the default Universal Time Coordinated (UTC) time zone.

After the configuration takes effect, the `display clock` command can be used to check it. Besides, the time of the log or debug information uses the local time after the adjustment of the time zone and summer time.

For the related command, see `clock summer-time`.

Example

```
# Set the name of the local time zone as Z5 with the time adding 5 hours compared with the UTC.
<Quidway> clock timezone z5 add 05:00:00
```

4.1.4 sysname

Syntax

```
sysname sysname
undo sysname
```

View

System view
Parameter

sysname: Specify the hostname with a character string with the length ranging from 1 to 30 characters.

Description

Using sysname command, you can configure the hostname of Ethernet Switch.

By default, the hostname of Ethernet Switch is Quidway.

Changing the hostname name of Ethernet Switch will affect the prompt of command line interface. E.g. the host name of Ethernet Switch is Quidway, and the prompt in user view is <Quidway>.

Example

# Set the hostname of the Ethernet Switch as QuidwayLANSwitch.
[Quidway] sysname QuidwayLANSwitch
[QuidwayLANSwitch]

4.2 System Status and System Information Display Commands

4.2.1 display clock

Syntax

display clock

View

Any view

Parameter

none

Description

Using display clock command, subscribers can obtain information about system data and time from the terminal display.

The maximum date and time the system can display is 23:59:59/9999/12/31.

For the related commands, see clock.

Example

# View the current system date and clock.
<Quidway> display clock
15:50:45 UTC Mon 2001/2/12
4.2.2  display current-configuration

Syntax

display  current-configuration  [  controller  |  interface  interface-type
[  interface-number  ]  |  configuration  [  post-system  |  system  |  user-interface  ]  ]  [  |
{  begin  |  exclude  |  include  }  regular-expression  ]

View

Any view

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: View the pre-positive and post-positive configuration information.
post-system: View the pre-positive configuration information.
system: View the configuration information of sysname.
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

Using display current-configuration command, you can display the currently effective 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, you can use the regular expression to filter the output information. For specific rules about the regular expression, refer to the corresponding operation manual.
For the related command, see save, reset saved-configuration and display saved-configuration.

Example

# View the running configuration parameters of the switch.
<Quidway> display current-configuration
#
  sysname S3026C
#
  radius scheme system
  server-type nec
  primary authentication 127.0.0.1 1645
  primary accounting 127.0.0.1 1646
  user-name-format without-domain

  domain system
  radius-scheme system
  access-limit disable
  state active
  idle-cut disable
  self-service-url disable
  messenger time disable

  domain default enable system
#
  local-server nas-ip 127.0.0.1 key nec
#
  interface Aux0/0
#
  vlan 1
#
  interface Ethernet0/1
#
  interface Ethernet0/2
#
  interface Ethernet0/3
#
  interface Ethernet0/4
#
  interface Ethernet0/5
#
  interface Ethernet0/6
# interface Ethernet0/7
# interface Ethernet0/8
# interface Ethernet0/9
# interface Ethernet0/10
# interface Ethernet0/11
# interface Ethernet0/12
# interface Ethernet0/13
# interface Ethernet0/14
# interface Ethernet0/15
# interface Ethernet0/16
# interface Ethernet0/17
# interface Ethernet0/18
# interface Ethernet0/19
# interface Ethernet0/20
# interface Ethernet0/21
# interface Ethernet0/22
# interface Ethernet0/23
# interface Ethernet0/24
# interface NULL0
# user-interface aux 0
user-interface vty 0 4
#
# View the lines containing the character string “10*” in the configuration information. The “*” indicates that the “0” before it can appear 0 times or multiple consecutive times.

```bash
<Quidway> display current-configuration | include 10*
```

primary authentication 127.0.0.1 1645
primary accounting 127.0.0.1 1646
local-server nas-ip 127.0.0.1 key nec

# View configuration information begin with “user”.

```bash
<Quidway> display current-configuration | include ^user
```

user-interface aux 0
user-interface vty 0 4

# View the pre-positive and post-positive configuration information.

```bash
<Quidway> display current-configuration configuration
```

```
#
sysname S3026C
#
radius scheme system
server-type nec
primary authentication 127.0.0.1 1645
primary accounting 127.0.0.1 1646
user-name-format without-domain
```

domain system
radius-scheme system
access-limit disable
state active
idle-cut disable
self-service-url disable

Huawei Technologies Proprietary
messenger time disable
domain default enable system
#
local-server nas-ip 127.0.0.1 key nec
#
vlan 1
#
user-interface aux 0
user-interface vty 0 4
#
return

4.2.3  display debugging

Syntax

display debugging  [ interface { interface-name | interface-type interface-num } ]
[ module-name ]

View

Any view

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

Using display debugging command, you can view 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.
<Quidway> display debugging
IP packet debugging switch is on.
4.2.4 display saved-configuration

Syntax

display saved-configuration

View

Any view

Parameter

none

Description

Using **display saved-configuration** command, you can view the configuration files in the flash memory of Ethernet Switch.

If the Ethernet Switch works abnormally after electrified, execute the **display saved-configuration** command to view the startup configuration of the Ethernet Switch.

For the related commands, see **save**, **reset saved-configuration**, **display current-configuration**.

Example

# Display configuration files in flash memory of Ethernet Switch.
<Quidway> display saved-configuration
#
  sysname S3026C
  
  radius scheme system
  server-type nec
  primary authentication 127.0.0.1 1645
  primary accounting 127.0.0.1 1646
  user-name-format without-domain

  domain system
  radius-scheme system
  access-limit disable
  state active
  idle-cut disable
  self-service-url disable
  messenger time disable

  domain default enable system
local-server nas-ip 127.0.0.1 key nec

interface Aux0/0

vlan 1

interface Ethernet0/1

interface Ethernet0/2

interface Ethernet0/3

interface Ethernet0/4

interface Ethernet0/5

interface Ethernet0/6

interface Ethernet0/7

interface Ethernet0/8

interface Ethernet0/9

interface Ethernet0/10

interface Ethernet0/11

interface Ethernet0/12

interface Ethernet0/13

interface Ethernet0/14

interface Ethernet0/15

interface Ethernet0/16

interface Ethernet0/17

interface Ethernet0/18
4.2.5  display users

Syntax

    display users [ all ]

View

    Any view

Parameter

    all: display all users connected to the switch.

Description

    Using display users command, you can view information about users connected to the switch.

Example

    # Display the status of the current users.
    <Quidway> display users
    UI   Delay   IPAddress    Username
    F 0 AUX 0  00:00:00
4.2.6  display version

Syntax

display version

View

Any view

Parameter

none

Description

Using display version command, you can view such information as software version, issue date and the basic hardware configurations.

Example

# Display the information about the system version.
<Quidway> display version
Versatile Routing Platform Software
VRP (R) Software, Version 3.10, RELEASE 0014
Copyright (c) Reserved.
S3026C uptime is 0 week,0 day,3 hours,13 minutes

64M    bytes SDRAM
8192K   bytes Flash Memory
Config Register points to FLASH

Hardware Version is REV.0
CPLD Version is 000
Bootrom Version is 120
[Subslot 0] 24 FE  Hardware Version is REV.0

4.3  System Debug Commands

4.3.1  debugging

Syntax

debugging { all | module-name [ debugging-option ] }
undo debugging { all | module-name [ debugging-option ] }
View

User view

Parameter

all: Enable or disable all the debugging.
module-name: Specify the module name.
debugging-option: Debugging option.

Description

Using debugging command, you can enable the system debugging. Using undo debugging command, you can disable the system debugging.

By default, all the debugging processes are disabled.

Ethernet 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. Specially, network system may collapse after all the debugging is enabled by debugging all command. So it is not suggested to use the debugging all command. It is convenient for the user to disable all the debugging with undo debugging all command.

For the related commands, see display debugging.

Example

# Enable IP Packet debugging.
<Quidway> debugging ip packet
IP packet debugging switch is on.

4.3.2 display diagnostic-information

Syntax

display diagnostic-information

View

Any view

Parameter

none
Description

Using **display diagnostic-information** command, you can view the current configuration information about all running modules. You can use all these information to help diagnose and troubleshoot the Ethernet switch.

When the Ethernet switch does not run well, you can collect all sorts of information about the switch to locate the source of fault. However, each module has its corresponding display command, which make it difficult for you to collect all the information needed. In this case, you can use **display diagnostic-information** command.

Example

```
# Display all system configuration information
<Quidway> display diagnostic-information
This operation may take a few minutes, continue?[Y/N]y
---------------display clock---------------
20:12:39 UTC Mon 2000/5/8
---------------display version---------------
Huawei Versatile Routing Platform Software
VRP (tm) software, Version 3.10
Copyright (c) 2000-2002 HUAWEI TECH CO., LTD.
```

4.4 Network Connection Test Commands

4.4.1 ping

Syntax

```
```

View

Any 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.
- **-f**: Drop the packets which are larger than the MTU instead of fragmenting them.
-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.

-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 of the destination host.

ip: Choose IP ICMP packet.

Description

Using ping command, you can 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 **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, you can increase the response message timeout.

For the related commands, see **tracert**.

### Example

```bash
# Check whether the host 202.38.160.244 is reachable.
<Quidway> 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
```

### 4.4.2 tracert

**Syntax**

```
tracert [ -a source-ip ] [ -f first-TTL ] [ -m max-TTL ] [ -p port ] [ -q num-packet ] [ -w timeout ] string
```

**View**

Any view

**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, num-packet is an integer specifying the number of query packets sent, larger than 0.

-w: Configure to verify the -wf 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**

Using `tracert` command, you can 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 `ping` command finds some error on the network, perform `tracert` to locate the error.

The output of `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.
<Quidway> 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
```

Huawei Technologies Proprietary
4.5 Log Commands

4.5.1 display channel

Syntax

display channel [channel-number | channel-name]

View

Any 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

Using display channel command, you can view the details about the information channel.

Without parameter, display channel command shows the configurations of all the channels.

Example

# Show details about the information channel 0.
4.5.2 display info-center

Syntax

display info-center

View

Any view

Parameter

None

Description

Using display info-center command, you can view 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.
<Quidway> 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

4.5.3 info-center channel name

Syntax

    info-center channel channel-number name channel-name

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

Using info-center channel name command, you can rename a channel specified by the channel-number as channel-name.
Note that the channel name cannot be duplicated.

Example

    # Rename the channel 0 as execconsole.
    [Quidway] info-center channel 0 name execconsole

4.5.4 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

Using info-center console channel command, you can configure the channel through which the log information is output to the console.

By default, Ethernet switches do 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.
[Quidway] info-center console channel 0

4.5.5 info-center enable

Syntax

info-center enable
undo info-center enable

View

System view

Parameter

none

Description

Using info-center enable command, you can enable the system log function. Using undo info-center enable command, you can 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.
    [Quidway] info-center enable

4.5.6  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); By default, the size of the buffer is 20.

Description

    Using info-center logbuffer command, you can configure to output information to the memory buffer. Using undo info-center logbuffer command, you can 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.
    [Quidway] info-center logbuffer size 50
4.5.7 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

Using `info-center loghost` command, you can configure the IP address of the info-center loghost to send information to it. Using `undo info-center loghost` command, you can cancel output to info-center loghost.

By default, Ethernet 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.
[Quidway] info-center loghost 202.38.160.1

4.5.8 info-center loghost source

Syntax

info-center loghost source interface-name

Example

# Configure to send log information to the UNIX workstation at 202.38.160.1.
[Quidway] info-center loghost 202.38.160.1
undo info-center loghost source

View

System view

Parameter

source interface-name: set source address of the packets sent to loghost as the address of the interface specified by the interface-name. Normally, the interface should be VLAN interface.

Description

Using info-center loghost source command, you can set source address of the packets sent to loghost as the address of the interface specified by the interface-name. Using undo info-center loghost source command, you can cancel the setting source address of the packets sent to loghost.

This command takes effect only after the system logging is enabled.

For the related commands, see info-center enable, display info-center.

Example

# Set source address of the packets sent to loghost as the address of the VLAN interface 1.

[Quidway] info-center loghost source vlan-interface 1

4.5.9  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

Using **info-center monitor channel** command, you can configure the channel to output the log information to the user terminal. Using **undo info-center monitor channel** command, you can restore the channel to output the log information to the user terminal to default value.

By default, Ethernet 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.
[Quidway] info-center monitor channel 0
```

**4.5.10 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

Using **info-center snmp channel** command, you can configure new channel for transmitting the SNMP information. Using **undo info-center snmp channel** command, you can restore the channel for transmitting the SNMP information to default value.

For the related commands, see **display snmp**.

Example

```
# Configure channel 6 as the SNMP information channel.
[Quidway] info-center snmp channel 6
```
4.5.11  info-center source

Syntax

```
info-center source  { modu-name | default } channel { channel-number | channel-name } [ { log | trap | debug } * { level severity | state state } * ]
undo info-center source  { modu-name | default } channel { channel-number | channel-name }
```

View

System view

Parameter

- **modu-name**: Module name.
- **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.

Information at different levels is as follows:

- **emergencies**: Level 0 information, which cannot be used by the system.
- **alerts**: Level 1 information, to be reacted immediately.
- **critical**: Level 2 information, critical information.
- **errors**: Level 3 information, error information.
- **warnings**: Level 4 information, warning information.
- **notifications**: Level 5 information, showed normally and important.
- **informational**: Level 6 information, notice to be recorded.
- **debugging**: Level 7 information, generated during the debugging progress.
- **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**.
Description

Using **info-center source** command, you can add/delete a record to the information channel. Using **undo info-center source** command, you can cancel 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 4-1 The default name of information channel

<table>
<thead>
<tr>
<th>Output direction</th>
<th>Information channel name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>console</td>
</tr>
<tr>
<td>Monitor</td>
<td>monitor</td>
</tr>
<tr>
<td>Info-center loghost</td>
<td>loghost</td>
</tr>
<tr>
<td>Log buffer</td>
<td>logbuf</td>
</tr>
<tr>
<td>Trap buffer</td>
<td>trapbuf</td>
</tr>
<tr>
<td>snmp</td>
<td>snmpagent</td>
</tr>
</tbody>
</table>

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 VLAN module in SNMP channel and allows the output of the information with a level higher than emergencies.

```
[Quidway] info-center source vlan channel snmp log level emergencies
```
4.5.12  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

Using `info-center switch-on` command, you can turn on the information synchronization switch of the specified switch. Using `undo info-center switch-on` command, you can turn off the information synchronization switch of the specified switch.

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

```
# Turn on the trapping information synchronization switch of the unit 2.
[Quidway] info-center switch 2 trapping
```
4.5.13 info-center timestamp

Syntax

```plaintext
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

Using `info-center timestamp` command, you can configure the timestamp output format in debugging/trap information. Using `undo info-center timestamp` command, you can disable the output of timestamp field.

By default, datetime stamp is used.

Example

```plaintext
# Configure the debugging information timestamp format as boot.
[Quidway] info-center timestamp debugging boot
```

4.5.14 info-center trapbuffer

Syntax

```plaintext
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

Using `info-center trapbuffer` command, you can output information to the trap buffer. Using `undo info-center trapbuffer` command, you can cancel output information to trap buffer.

By default, output information is transmitted to trap buffer and size of trap buffer is 20.

This command takes effect only after the system logging is enabled.

For the related commands, see `info-center enable`, `display info-center`.

Example

```
# Send information to the trap buffer and sets the size of buffer as 30.
[Quidway] info-center trapbuffer size 30
```

4.5.15 reset logbuffer

Syntax

`reset logbuffer`

View

User view

Parameter

- **none**

Description

Using `reset logbuffer` command, you can reset information in log buffer.

Example

```
# Clear information in log buffer.
<Quidway> reset logbuffer
```
4.5.16  reset trapbuffer

Syntax

reset trapbuffer

View

User view

Parameter

none

Description

Using reset trapbuffer command, you can reset information in trap buffer.

Example

# Clear information in trap buffer.
<Quidway> reset trapbuffer

4.5.17  terminal debugging

Syntax

terminal debugging
undo terminal debugging

View

User view

Parameter

none

Description

Using terminal debugging command, you can configure to display the debugging information on the terminal. Using undo terminal debugging command, you can configure not to display the debugging information on the terminal.

By default, the displaying function is disabled.

For the related commands, see debugging.

Example

# Enable the terminal display debugging.
<Quidway> terminal debugging
4.5.18 terminal logging

Syntax

    terminal logging
    undo terminal logging

View

    User view

Parameter

    none

Description

    Using `terminal logging` command, you can enable terminal log information display. Using `undo terminal logging` command, you can disable terminal log information display.

    By default, this function is enabled.

Example

    # Disable the terminal log display.
    <Quidway> undo terminal logging

4.5.19 terminal monitor

Syntax

    terminal monitor
    undo terminal monitor

View

    User view

Parameter

    none

Description

    Using `terminal monitor` command, you can enable the log debugging/log/trap on the terminal monitor. Using `undo terminal monitor` command, you can 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 undo terminal debugging,undo terminal logging,undo terminal trapping commands. When the terminal monitor is enabled, you can 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.
<Quidway> undo terminal monitor

4.5.20 terminal trapping

Syntax

terminal trapping
undo terminal trapping

View

User view

Parameter

none

Description

Using terminal trapping command, you can enable terminal trap information display. Using undo terminal trapping command, you can disable this function.

By default, this function is enabled.

Example

# Enable trap information display.
<Quidway> terminal trapping
Chapter 5  SNMP Configuration Commands

5.1  SNMP Configuration Commands

5.1.1  display snmp-agent community

Syntax

display snmp-agent community [ read | write ]

View

Any view

Parameter

read: display read-only community information.
write: display read-write community information.

Description

Using display snmp-agent community command, you can view the currently configured community names.

Example

# Display the currently configured community names.
<Quidway> display snmp-agent community
community name:public
group name:public
storage-type: nonVolatile

community name:tom
group name:huawei
storage-type: nonVolatile

5.1.2  display snmp-agent

Syntax

display snmp-agent { local-engineid | remote-engineid }

View

Any view
Parameter

**local-engineid**: local engine ID.

**remote-engineid**: remote engine ID.

Description

Using `display snmp-agent engineid` command, you can view 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

```plaintext
# Display the engine ID of current device.
<Quidway> display snmp-agent local-engineid
SNMP local engineID: 00000009020000000C025808
```

5.1.3 `display snmp-agent group`

Syntax

`display snmp-agent group [ group-name ]`

View

Any view

Parameter

**groupname**: Group name, ranging from 1 to 32 bytes.

Description

Using `display snmp-agent group` command, you can view group name, safe mode, state of various views and storage modes.

Example

```plaintext
# Display SNMP group name and safe mode.
<Quidway> display snmp-agent group
Group name: huawei
Security model: v2c noAuthnoPriv
Readview: ViewDefault
Writeview: <no specified>
Notifyview: <no specified>
Storage-type: nonVolatile
```

The following table describes the output fields.
Table 5-1 Output description of the display snmp-agent group command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupname</td>
<td>SNMP Group name of the user</td>
</tr>
<tr>
<td>Security model</td>
<td>The security model adopted by SNMP</td>
</tr>
<tr>
<td>readview</td>
<td>Read-only MIB view name corresponding to that group</td>
</tr>
<tr>
<td>writeview</td>
<td>Writable MIB view corresponding to that group</td>
</tr>
<tr>
<td>notifyview</td>
<td>The name of the notify MIB view corresponding to that group</td>
</tr>
<tr>
<td>storage-type</td>
<td>Storage type</td>
</tr>
</tbody>
</table>

5.1.4 display snmp-agent mib-view

Syntax

```plaintext
display snmp-agent mib-view [ exclude | include | { viewname mib-view } ]
```

View

Any view

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 Ethernet switch.

Example

```plaintext
# Display the information about the currently configured MIB view.
<Quidway> display snmp-agent mib-view
View name:mv MIB Subtree:internet
Storage-type: nonVolatile -included active

View name:test MIB Subtree:internet
Storage-type: nonVolatile -included active

View name:ViewDefault MIB Subtree:internet
Storage-type: nonVolatile -included active
```
View name: ViewDefault     MIB Subtree: snmpUsmMIB  
Storage-type: nonVolatile  -excluded active

View name: ViewDefault     MIB Subtree: snmpVacmMIB  
Storage-type: nonVolatile  -excluded active

View name: ViewDefault     MIB Subtree: snmpModules.18  
Storage-type: nonVolatile  -excluded active

The following table describes the output fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View name</td>
<td>View name</td>
</tr>
<tr>
<td>MIB Subtree</td>
<td>MIB subtree</td>
</tr>
<tr>
<td>storage-type</td>
<td>Storage type</td>
</tr>
<tr>
<td>included/excluded</td>
<td>Permit or forbid access to an MIB object</td>
</tr>
<tr>
<td>active</td>
<td>Indicate the line state in the table</td>
</tr>
</tbody>
</table>

**Caution:**
If the SNMP Agent is disabled, "Snmp Agent disabled" will be displayed after you execute the above display commands.

### 5.1.5 display snmp-agent statistics

**Syntax**

display snmp-agent statistics

**View**

Any view

**Parameter**

none
Description

Using **display snmp-agent statistics** command, you can view current state of SNMP communication.

This command provides a counter for SNMP operations.

Example

```bash
# Display the current state of SNMP communication.
<Quidway> display snmp-agent statistics
9 Messages delivered to the SNMP entity
0 Messages which were for an unsupported version
0 Messages which used a SNMP community name not known
0 Messages which represented an illegal operation for the community supplied
0 ASN.1 or BER errors in the process of decoding
9 Messages passed from the SNMP entity
0 SNMP PDUs which had badValue error-status
0 SNMP PDUs which had genErr error-status
0 SNMP PDUs which had noSuchName error-status
0 SNMP PDUs which had tooBig error-status (Maximum packet size 1500)
9 MIB objects retrieved successfully
0 MIB objects altered successfully
0 GetRequest-PDU accepted and processed
9 GetNextRequest-PDU accepted and processed
9 GetResponse-PDU accepted and processed
0 SetRequest-PDU accepted and processed
0 Trap PDUs accepted and processed
```

5.1.6 **display snmp-agent sys-info contact**

Syntax

```bash
display snmp-agent sys-info contact
```

View

Any view

Parameter

none

Description

Using **display snmp-agent sys-info contact** command, you can view the character string sysContact (system contact).
Example

# Display the character string sysContact (system contact).
<Quidway> display snmp-agent sys-info contact
The contact person for this managed node:
Mr. Wang- Tel: 3306

5.1.7 display snmp-agent sys-info location

Syntax

display snmp-agent sys-info location

View

Any view

Parameter

none

Description

Using display snmp-agent sys-info location command, you can view the character string describing the system location.

Example

# Display the system location.
<Quidway> display snmp-agent sys-info location
The physical location of this node:
BeiJing China

5.1.8 display snmp-agent sys-info version

Syntax

display snmp-agent sys-info version

View

Any view

Parameter

none

Description

Using display snmp-agent sys-info version command, you can view the version information about the running SMNMP in the system.
Example

```
# Display the version information of running SNMP
<Quidway> display snmp-agent sys-info version
SNMP version running in the system:
SNMPv3
```

5.1.9 display snmp-agent usm-user

Syntax

```
display snmp-agent usm-user [ engineid engineid ] [ group groupname ] [ username username ]
```

View

Any view

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

Using `display snmp-agent usm-user` command, you can view information of all the SNMP usernames in the group username list.

Example

```
# Display the information of all the current users.
<Quidway> display snmp-agent usm-user
User name: authuser
Engine ID: 00000009020000000C025808
UserStatus: active
```

The following table describes the output fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Name of SNMP user</td>
</tr>
<tr>
<td>Engine ID</td>
<td>Character string identifying SNMP device</td>
</tr>
<tr>
<td>UserStatus</td>
<td>The status of the user, may be active or inactive.</td>
</tr>
</tbody>
</table>
5.1.10 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 including; By default, the value is "Enterprise Number +
device information".

Description

Using `snmp-agent local-engineid` command, you can configure a name for a local or
remote SNMP engine on the Ethernet Switch. Using `undo snmp-agent
local-engineid` command, you can 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 12345.
<Quidway> display snmp-agent local-engineid
```

5.1.11 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

Using **snmp-agent community** command, you can configure community access name and enable the access to SNMP. Using **undo snmp-agent community** command, you can cancel the settings of community access name.

Example

# Configure community name as huawei and permits read-only access by this community name.
[Quidway] snmp-agent community read huawei

# Configure community name as mgr and permits read-write access.
[Quidway] snmp-agent community write mgr

5.1.12 **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

**groupname**: Group name, ranging from 1 to 32 bytes.

**authentication**: Configure to authenticate the packet without encryption.

**privacy**: Configure to authenticate and encrypt the packet.

**read-view**: Configures to allow read-only view settings.

**readview**: Read-only view name, ranging from 1 to 32 bytes.

**write-view**: Configure to allow read-write view settings.

**writeview**: Name of read-write view, ranging from 1 to 32 bytes.

**notify-view**: Configure to allow notify view settings.
notifyview: Specify the notify view name, ranging from 1 to 32 bytes.

acl acl-list: Set access control list for this group name.

Description

Using `snmp-agent group` command, you can configure a new SNMP group, that is, to map SNMP user to SNMP view. Using `undo snmp-agent group` command, you can cancel a specified SNMP group.

For the following reasons:

- `snmp-agent target-host` command automatically generates a `notifyview` for 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.

Please do not specify the notify view when configuring SNMP group.

Example

```
# Create an SNMP group named huawei.
[Quidway] snmp-agent group v3 huawei.
```

5.1.13  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

Using `snmp-agent mib-view` command, you can create or update the view information. Using `undo snmp-agent mib-view` command, you can cancel 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.

[Quidway] snmp-agent mib-view included mib2 5.6.1.3

5.1.14 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. By default, the size is 1500 bytes.

Description

Using `snmp-agent packet max-size` command, you can configure the size of SNMP packet that the Agent can send/receive. Using `undo snmp-agent packet max-size` command, you can restore the default size of SNMP packet.

The sizes of the SNMP packets received/sent by the Agent are different in different network environment.

Example

# Set the size of SNMP packet to 1042 bytes.

[Quidway] snmp-agent packet max-size 1042

5.1.15 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 maintaining contact (in bytes), with a length ranging from 1 to 255; By default, the contact information is "HuaWei Beijing China".
- **sysLocation**: Specify a character string to describe the system location; By default, the character string is "Beijing China".
- **version**: version of running SNMP. By default, the version is SNMP V3.
  - **v1**: SNMP V1.
  - **v2c**: SNMP V2C.
  - **v3**: SNMP V3.
  - **all**: all SNMP version (includes SNMP V1, SNMP V2C, SNMP V3).

Description

Using **snmp-agent sys-info** command, you can configure system information such as geographical location of the device, contact information for system maintenance and version information of running SNMP. Using **undo snmp-agent sys-info location** command, you can restore the default value.

By default, the contact information is "HuaWei Beijing China", the system location is "Beijing China", the SNMP version is SNMP V3.

Example

```shell
# Set system location as Building 3/Room 214.
[Quidway] snmp-agent sys-info location Building 3/Room 214
```

5.1.16 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**: Specify the host to receive traps or notifications
- **address**: Specify the transport addresses to be used in the generation of SNMP messages.

Huawei Technologies Proprietary

5-12
udp-domain: Specify transport domain over UDP for the target address

host-addr: IP address of destination host.

udp-port udp-port-number: Specify the UDP port number of the host to receive the SNMP notification.

params: Specify SNMP target information to be used in the generation of SNMP messages

v1: Represent the version of SNMPV1.

v2c: Represent the version of SNMPV2C.

v3: Represent the version of SNMPV3.

authentication: Configure to authenticate the packet without encryption.

privacy: Configure to authenticate and encrypt the packet.

community-string: Specify the community name. The character string ranges from 1 to 32 bytes.

Description

Using snmp-agent target-host command, you can configure destination of SNMP notification. Using undo snmp-agent target-host command, you can cancel the host that receives SNMP notification.

The snmp-agent target-host command and the snmp-agent trap enable command should be used at the same time. Use the snmp-agent trap enable command to enable the device to transmit Trap packets. snmp-agent trap enable command and snmp-agent target-host command should be used at the same time on the host to enable notify message sending.

Example

# Enable sending Trap message to myhost.huawei.com with community name huawei.
[Quidway] snmp-agent trap enable
[Quidway] snmp-agent target-host trap address udp-domain 2.2.2.2 params securityname huawei

# Enable sending Trap packets to 2.2.2.2 with the community name public
[Quidway] snmp-agent trap enable
[Quidway] snmp-agent target-host trap address udp-domain 2.2.2.2 params securityname public

5.1.17 snmp-agent trap enable

Syntax

snmp-agent trap enable [ standard [ authentication ] [ coldstart ] [ linkdown ] [ linkup ] [ warmstart ] ]
undo snmp-agent trap enable [ standard [ authentication ] [ coldstart ] [ linkdown ] [ linkup ] [ warmstart ] ]

View

System view

Parameter

standard [ authentication ] [ coldstart ] [ linkdown ] [ linkup ] [ warmstart ]:
Configure to send standard Trap messages. authentication: Configure to send SNMP authentication Trap messages. coldstart: Configure to send SNMP cold start Trap messages. linkdown: Configure to send SNMP link down Trap messages. linkup: Configure to send SNMP link up Trap messages. warmstart: Configure to send SNMP warm start Trap messages.

Description

Using snmp-agent trap enable command, you can enable the device to send Trap message. Using undo snmp-agent trap enable command, you can disable Trap message sending.

By default, Trap message sending is disabled.

snmp-agent trap enable command and snmp-agent target-host command should be used at the same time. snmp-agent target-host command specifies which hosts can receive Trap message. However, to send Trap message, 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 huawei.
[Quidway] snmp-agent trap enable standard authentication
[Quidway] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname huawei

5.1.18 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

Using `snmp-agent trap life` command, you can configure the timeout of Trap packets. Using `undo snmp-agent trap life` command, you can 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.

[Quidway] snmp-agent trap life 60

5.1.19 `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; By default, the length is 100.

Description

Using `snmp-agent trap queue-size` command, you can configure the information queue length of Trap packet sent to destination host. Using `undo snmp-agent trap queue-size` command, you can 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.

[Quidway] snmp-agent trap queue-size 200
5.1.20 snmp-agent trap source

**Syntax**

```plaintext
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 4000.

**Description**

Using **snmp-agent trap source** command, you can configure the source address for sending Trap. Using **undo snmp-agent trap source** command, you can cancel the source address for sending Trap.

**Example**

```plaintext
# Configure the IP address of the VLAN interface 1 as the source address for transmitting the Trap packets.
[Quidway] snmp-agent trap source vlan-interface 1
```

5.1.21 snmp-agent usm-user

**Syntax**

```plaintext
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`: Specify the user name, ranging from 1 to 32 bytes.
- `groupname`: Specify the group name corresponding to that user, a character string at the length ranging from 1 to 32 bytes.
- `v1`: Configure to use V1 safe mode.
- `v2c`: Configure to use V2c safe mode.
v3: Configure to use V3 safe mode.

**authentication-mode**: Specify the safety level as authentication required.

**md5**: MD5 algorithm is adopted in authentication. MD5 authentication uses the 128-digit password. Computation speed of MD5 is faster than that of SHA.

**sha**: SHA algorithm is adopted in authentication. SHA authentication uses the 160-digit password. Computation speed of SHA is slower than that of MD5, but with higher security.

**authpassword**: Specify the authentication password with a character string, ranging from 1 to 64 bytes.

**privacy-mode**: Specify the safety level as encrypted.

**des56**: Specify the authentication protocol as DES.

**privpassword**: Specify the encryption password with a character string, ranging from 1 to 64 bytes.

**acl acl-list**: Set access control list for this user based on USM name

**Description**

Using `snmp-agent usm-user` command, you can add a new user to an SNMP group. Using `undo snmp-agent usm-user` command, you can cancel a user from SNMP group.

SNMP engineID (for authentication) is required when configuring remote user for an agent. This command will not be effective without engineID 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.

**Example**

```
# Add a user wang for huawei (an SNMP group), configures to authenticate with MD5 and sets authentication password as pass.
[Quidway] snmp-agent usm-user v3 wang huawei authentication-mode md5 pass
```

### 5.1.22 undo snmp-agent

**Syntax**

`undo snmp-agent`

**View**

System view

**Parameter**

none
Description

Using **undo snmp-agent** command, you can disable all versions of SNMP running on the server.

Perform any command of **snmp-agent** will enable SNMP Agent.

Example

# Disable the running SNMP agents of all SNMP versions.

[Quidway] undo snmp-agent
Chapter 6  RMON Configuration Commands

6.1  RMON Configuration Commands

6.1.1  display rmon alarm

Syntax

display rmon alarm [ alarm-table-entry ]

View

Any view

Parameter

alarm-table-entry: Alarm table entry index.

Description

Using display rmon alarm command, you can view RMON alarm information.
For the related commands, see rmon alarm.

Example

# Display the RMON alarm information.
<Quidway> display rmon alarm
Alarm table 1 owned by HUAWEI 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 6-1  Output description of the display rmon alarm command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm table 1</td>
<td>Index 1 in the alarm table</td>
</tr>
<tr>
<td>HUAWEI</td>
<td>Owner</td>
</tr>
<tr>
<td>VALID</td>
<td>The entry corresponding to the index is valid</td>
</tr>
<tr>
<td>Samples absolute value</td>
<td>Sampling the absolute value of the node 1.3.6.1.2.1.16.1.1.1.4.1</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Sampling interval | The interval of sampling the value
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.
startup | The first trigger
risingOrFallingAlarm | The type of the first alarm: Specifies to alarm when exceeding the rising threshold or the falling threshold

### 6.1.2 display rmon event

**Syntax**

```
display rmon event [ event-table-entry ]
```

**View**

Any view

**Parameter**

- `event-table-entry`: Entry index of event table.

**Description**

Using `display rmon event` command, you can 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).

For the related commands, see `rmon event`.

**Example**

```
# Show the RMON event.
<Quidway> display rmon event
Event table 1 owned by HUAWEI is VALID.
    Description: null.
    Will cause log-trap when triggered, last triggered at 0days 00h:02m:27s.
```
Table 6-2 Output description of the display rmon event command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event table 1</td>
<td>Index 1 in event table</td>
</tr>
<tr>
<td>HUAWEI</td>
<td>Owner</td>
</tr>
<tr>
<td>VALID</td>
<td>The entry corresponding to the index is valid</td>
</tr>
<tr>
<td>Description</td>
<td>Event description</td>
</tr>
<tr>
<td>Will cause log-trap when</td>
<td>When the event is triggered, it will cause the log-trap. And the last</td>
</tr>
<tr>
<td>triggered, last triggered at</td>
<td>triggered time is 00h:02m:27s</td>
</tr>
<tr>
<td>0days 00h:02m:27s</td>
<td></td>
</tr>
</tbody>
</table>

6.1.3 display rmon eventlog

Syntax

```
display rmon eventlog [ event-number ]
```

View

Any view

Parameter

`event-number`: Entry index of event table.

Description

Using `display rmon eventlog` command, you can view 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 centisecond).

Example

```
# Show event log of RMON.
<Quidway> display rmon eventlog 1
Event table 1 owned by HUAWEI 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 6-3 Output description of the display rmon eventlog command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event table 1</td>
<td>Index 1 in event table</td>
</tr>
<tr>
<td>HUAWEI</td>
<td>Owner</td>
</tr>
<tr>
<td>VALID</td>
<td>The entry corresponding to the index is valid</td>
</tr>
<tr>
<td>Description</td>
<td>Event description</td>
</tr>
<tr>
<td>less than(or =) 100 with alarm value 0</td>
<td>The alarm sample value is less than or equal to 100</td>
</tr>
<tr>
<td>Alarm sample type is absolute</td>
<td>The type of alarm sampling is absolute</td>
</tr>
<tr>
<td>Generates eventLog 1.2 at 0days 00h:02m:27s</td>
<td>The eventlog corresponding to the index 1.2 is generated at 0days 00h:02m:27s.</td>
</tr>
</tbody>
</table>

#### 6.1.4 display rmon history

**Syntax**

```plaintext
display rmon history [ port-num ]
```

**View**

Any view

**Parameter**

`port-num`: Ethernet port name.

**Description**

Using `display rmon history` command, you can view 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.
<Quidway> display rmon history ethernet 2/1
History control entry 1 owned by HUAWEI is VALID
Samples interface : Ethernet2/1<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
```

Huawei Technologies Proprietary
undersize packets :0 , oversize packets :0
fragments :0 , jabbers :0
collisions :0 , utilization :0

Table 6-4 Output description of the display rmon history command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>History control entry</td>
<td>Index number in history control table</td>
</tr>
<tr>
<td>HUAWEI</td>
<td>Owner</td>
</tr>
<tr>
<td>VALID</td>
<td>The entry corresponding to the index is valid</td>
</tr>
<tr>
<td>Samples interface</td>
<td>The sampled interface</td>
</tr>
<tr>
<td>Sampling interval</td>
<td>Sampling interval</td>
</tr>
<tr>
<td>buckets</td>
<td>Records in history control table</td>
</tr>
<tr>
<td>dropevents</td>
<td>Dropping packet events</td>
</tr>
<tr>
<td>octets</td>
<td>Sent/Received octets in sampling time</td>
</tr>
<tr>
<td>packets</td>
<td>Packets sent/received in sampling time</td>
</tr>
<tr>
<td>broadcast packets</td>
<td>Number of broadcast packets</td>
</tr>
<tr>
<td>multicast packets</td>
<td>Number of multicast packets</td>
</tr>
<tr>
<td>CRC alignment errors</td>
<td>Number of CRC error packets</td>
</tr>
<tr>
<td>undersized packets</td>
<td>Number of undersized packets</td>
</tr>
<tr>
<td>oversized packets</td>
<td>Number of oversized packets</td>
</tr>
<tr>
<td>fragments</td>
<td>Number of undersized and CRC error packets</td>
</tr>
<tr>
<td>jabbers</td>
<td>Number of oversized and CRC error packets</td>
</tr>
<tr>
<td>collisions</td>
<td>Number of collision packets</td>
</tr>
<tr>
<td>utilization</td>
<td>Utilization</td>
</tr>
</tbody>
</table>

6.1.5  display rmon prialarm

Syntax

display rmon prialarm [ prialarm-table-entry ]

View

Any view

Parameter

prialarm-table-entry:entry of extended alarm table.
Description

Using **display rmon prialarm** command, you can view information about extended alarm table.

For the related commands, see **rmon prialarm**.

Example

```
# display alarm information about extended RMON.
<Quidway> display rmon prialarm
Prialarm table 1 owned by HUAWEI 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 6-5** Output description of the display rmon prialarm command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prialarm table 1</td>
<td>Index of extended alarm entry.</td>
</tr>
<tr>
<td>owned by HUAWEI</td>
<td>Creator of the extended alarm entry.</td>
</tr>
<tr>
<td>VALID</td>
<td>The entry corresponding to the index is valid.</td>
</tr>
<tr>
<td>Samples absolute value</td>
<td>Sampling the absolute value of the node 1.3.6.1.2.1.16.1.1.1.4.1.</td>
</tr>
<tr>
<td>Rising threshold</td>
<td>Rising threshold. When sampling value rises from normal value to this threshold, rising threshold alarm will be triggered.</td>
</tr>
<tr>
<td>Falling threshold</td>
<td>Falling threshold. When sampling value decreases from normal value to this threshold, falling threshold alarm will be triggered.</td>
</tr>
<tr>
<td>linked with event 1</td>
<td>Corresponding event index of ring and falling threshold alarm.</td>
</tr>
<tr>
<td>When startup enables:</td>
<td>Kind of first alarm. It may trigger rising threshold alarm or falling threshold alarm or both.</td>
</tr>
<tr>
<td>risingOrFallingAlarm</td>
<td></td>
</tr>
<tr>
<td>This entry will exist forever</td>
<td>The lifespan of this alarm entry which can be forever or a specified period of time.</td>
</tr>
<tr>
<td>Latest value : 0</td>
<td>The value of the latest sampling.</td>
</tr>
</tbody>
</table>
6.1.6  display rmon statistics

Syntax

display rmon statistics [ port-num ]

View

Any view

Parameter

port-num: Ethernet port number.

Description

Using display rmon statistics command, you can view 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.

For the related commands, see rmon statistics.

Example

# Show RMON statistics.

<Quidway> display rmon statistics Ethernet 2/1
Statistics entry 1 owned by HUAWEI is VALID.

Interface: Ethernet2/1<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 6-6  Output description of the display rmon statistics command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Port</td>
</tr>
<tr>
<td>HUAWEI</td>
<td>Owner</td>
</tr>
<tr>
<td>VALID</td>
<td>The entry corresponding to the index is valid</td>
</tr>
<tr>
<td>octets</td>
<td>Received/Sent octets in sampling time</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
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

### 6.1.7 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

Using rmon alarm command, you can add an entry to the alarm table. Using undo rmon alarm command, you can cancel 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.
[Quidway] undo rmon alarm 15

6.1.8 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: Name of the community that trap message is sent to.
log-trap: Log and trap event.
log-trapcommunity: Name of the community that 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

Using `rmon event` command, you can add an entry to the event table. Using `undo rmon event` command, you can cancel 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 marks it as log event.
[Quidway] rmon event 10 log

6.1.9 `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 to 127.

Description

Using `rmon history` command, you can add an entry to the history control table. Using `undo rmon history` command, you can cancel 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.
[Quidway-Ethernet0/1] undo rmon history 15
6.1.10 rmon prialarm

Syntax

```plaintext
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 ]
```

```plaintext
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

Using `rmon prialarm` command, you can add an entry to the extended RMON alarm table. Using `undo rmon prialarm` command, you can cancel 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.
[Quidway] undo rmon prialarm 10

6.1.11 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 to 127.

Description

Using rmon statistics command, you can add an entry to the statistic table. Using undo rmon statistics command, you can cancel 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 entry 20 to the statistics table of Ethernet1/1.
[Quidway-ethernet1/1] rmon statistic 20
Chapter 7  NTP Configuration Commands

7.1  NTP Configuration Commands

7.1.1  debugging ntp-service

**Syntax**

debugging ntp-service { access | adjustment | authentication | event | filter | packet | parameter | refclock | selection | synchronization | validity | all }

undo debugging ntp-service { access | adjustment | authentication | event | filter | packet | parameter | refclock | selection | synchronization | validity | all }

**View**

User view

**Parameter**

- **access**: NTP access control debugging.
- **adjustment**: NTP clock adjustment debugging.
- **all**: All NTP debugging functions.
- **authentication**: NTP authentication debugging.
- **event**: NTP event debugging.
- **filter**: NTP filter information debugging.
- **packet**: NTP packet debugging.
- **parameter**: NTP clock parameter debugging.
- **refclock**: NTP reference clock debugging.
- **selection**: NTP clock selection information debugging.
- **synchronization**: NTP clock synchronization information debugging.
- **validity**: NTP remote host validity debugging.

**Description**

Using **debugging ntp-service** command, you can debug different NTP services. Using **undo debugging ntp-service** command, you can disable corresponding debugging function.

By default, no debugging function is enabled.
Example

# Enable NTP access control debugging.
<Quidway> debugging ntp-service access

7.1.2 display ntp-service sessions

Syntax

display ntp-service sessions [ verbose ]

View

Any view

Parameter

verbose: Indicate to display the detail information about the sessions.

Description

Using display ntp-service sessions command, you can display the status of all the sessions maintained by NTP service provided by the local equipment.

By default, the status of all the sessions maintained by NTP service provided by the local equipment will be displayed.

When you configure this command without the verbose parameter, the Ethernet switch will display the brief information about all the sessions it maintains.

With the verbose parameter configured, Ethernet switch will display the detail information about all the sessions it maintains.

Example

# Display the status of all the sessions maintained by NTP service.
<Quidway> display ntp-service sessions
source refid st now poll reach delay offset disp
********************************************************************
[12345]212.125.95.4 131.188.3.221 2 18 64 377 339.8 10.8 0.9
note: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured

7.1.3 display ntp-service status

Syntax

display ntp-service status

View

Any view
Parameter

None

Description

Using command **display ntp-service status**, you can display the NTP service status.

Example

# Display the NTP service status.

```
<Quidway> 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)
```

The following table describes the outputs:

<table>
<thead>
<tr>
<th>Output</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>clock status: unsynchronized</td>
<td>Local clock status: do not synchronize to any remote NTP server.</td>
</tr>
<tr>
<td>clock stratum: 16</td>
<td>Indicates the NTP stratum of local clock.</td>
</tr>
<tr>
<td>reference clock ID</td>
<td>Indicates the address of a remote server of the reference ID, in the case that the local system has been synchronized by a remote NTP server or the ID of some clock source.</td>
</tr>
<tr>
<td>nominal frequency</td>
<td>Nominal frequency of the local system hardware clock</td>
</tr>
<tr>
<td>actual frequency</td>
<td>Actual frequency of the local system hardware clock.</td>
</tr>
<tr>
<td>clock precision</td>
<td>Precision of local system clock</td>
</tr>
<tr>
<td>clock offset</td>
<td>Offset of the local clock to the NTP server clock</td>
</tr>
<tr>
<td>root delay</td>
<td>Root delay from local equipment to the master reference clock.</td>
</tr>
<tr>
<td>root dispersion</td>
<td>Dispersion of the local clock relative to the NTP server clock</td>
</tr>
<tr>
<td>peer dispersion</td>
<td>Dispersion of the remote NTP server.</td>
</tr>
<tr>
<td>reference time</td>
<td>Reference timestamp</td>
</tr>
</tbody>
</table>
7.1.4 display ntp-service trace

Syntax

    display ntp-service trace [ ip-address ]

View

    Any view

Parameter

    ip-address: Specify the IP address of the NTP server serving as the reference clock source.

Description

Using `display ntp-service trace` command, you can display the brief information about every NTP server on the way from the local equipment to the reference clock source.

Example

    # Display the brief information about every NTP server.
    <Quidway> display ntp-service trace
    server 127.0.0.1,stratum 8, offset 0.000000, synch distance 0.00000
    refid 127.127.1.0

7.1.5 ntp-service access

Syntax

    ntp-service access { query | synchronization | server | peer } acl-number
    undo ntp-service access { query | synchronization | server | peer }

View

    System view

Parameter

    query: Allow to control query authority.
    synchronization: Only allow the server to access.
    server: Allow query to server and access.
    peer: Full access authority.

    acl-number: IP address list number, ranging from 2000 to 2999.
Description

Using `ntp-service access` command, you can set the authority to access the local equipment. Using `undo ntp-service access` command, you can cancel the access authority settings.

By default, there is no limit to the access.

Set authority to access the NTP services on a local Ethernet Switch. This is a basic and brief security measure, compared to authentication. An access request will be matched with `peer`, `serve`, `serve only`, and `query only` in an ascending order of the limitation. The first matched authority will be given.

Example

# Give the authority of time request, query control and synchronization with the local equipment to the peer in ACL 2076.
[Quidway] ntp-service access peer 2076

# Give the authority of time request and query control of the local equipment to the peer in ACL 2028.
[Quidway] ntp-service access synchronization 2028

7.1.6 ntp-service authentication enable

Syntax

    ntp-service authentication enable
    undo ntp-service authentication enable

View

    System view

Parameter

    None

Description

Using `ntp-service authentication enable` command, you can enable the NTP-service authentication function. Using `undo ntp-service authentication enable` command, you can disable this function.

By default, the authentication is disabled.

Example

# Enable NTP authentication function.
[Quidway] ntp-service authentication enable
7.1.7  ntp-service authentication-keyid

Syntax

ntp-service authentication-keyid number authentication-mode md5 value
undo ntp-service authentication-keyid number

View

System view

Parameter

number: Specify the key number and range from 1 to 4294967295.
value: Specify the value of the key with 1 to 32 ASCII characters.

Description

Using ntp-service authentication-keyid command, you can set NTP authentication key. Using undo ntp-service authentication-keyid command, you can cancel the NTP authentication key.

By default, there is no authentication key.

Only MD5 authentication is supported for the NTP authentication key settings.

Example

# Set MD5 authentication key 10 as BetterKey.
[Quidway] ntp-service authentication-keyid 10 authentication-mode md5 BetterKey

7.1.8  ntp-service broadcast-client

Syntax

ntp-service broadcast-client
undo ntp-service broadcast-client

View

VLAN interface view

Parameter

None
Description

Using `ntp-service broadcast-client` command, you can configure NTP broadcast client mode. Using `undo ntp-service broadcast-client` command, you can disable the NTP broadcast client mode.

By default, the NTP broadcast client mode is disabled.

Designate an interface on the local Ethernet Switch to receive NTP broadcast messages and operate in broadcast client mode. The local Ethernet Switch listens to the broadcast from the server. When it receives the first broadcast packet, it starts a brief client/server mode to switch messages with a remote server for estimating the network delay. Thereafter, the local Ethernet Switch enters broadcast client mode and continues listening to the broadcast and synchronizes the local clock according to the arrived broadcast message.

Example

```
# Configure to receive NTP broadcast packets via Vlan-Interface1.
[Quidway] interface vlan-interface1
[Quidway-Vlan-Interface1] ntp-service broadcast-client
```

7.1.9 ntp-service broadcast-server

Syntax

```
ntp-service broadcast-server [ authentication-keyid keyid version number ]
undo ntp-service broadcast-server
```

View

VLAN interface view

Parameter

`authentication-keyid`: Specify the authentication key.

`keyid`: Key ID used in broadcast, ranging from 0 to 4294967295.

`version`: Define NTP version number.

`number`: NTP version number, ranging from 1 to 3.

Description

Using `ntp-service broadcast-server` command, you can configure NTP broadcast server mode. Using `undo ntp-service broadcast-server` command, you can disable the NTP broadcast server mode.

By default, the broadcast service is disabled and `number` defaults to 3.
Designate an interface on the local equipment to broadcast NTP packets. The local equipment runs in broadcast-server mode and regularly broadcasts packets to its clients.

Example

# Configure to broadcast NTP packets via Vlan-Interface1 and encrypt them with Key 4 and set the NTP version number as 3.

[Quidway] interface vlan-interface1
[Quidway-Vlan-Interface1] ntp-service broadcast-server authentication-key 4 version 3

7.1.10 ntp-service max-dynamic-sessions

Syntax

ntp-service max-dynamic-sessions number
undo ntp-service max-dynamic-sessions

View

System view

Parameter

number: The maximum sessions can be created locally, ranging from 0 to 100.

Description

Using ntp-service max-dynamic-sessions command, you can set how many sessions can be created locally. Using undo ntp-service max-dynamic-sessions command, you can resume the default maximum session number

By default, a local device allows up to 100 sessions.

Example

# Set the local equipment to allow up to 50 sessions.

[Quidway] ntp-service max-dynamic-sessions 50

7.1.11 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*: Specify an multicast IP address of Class D.

**Description**

Using `ntp-service multicast-client` command, you can configure the NTP multicast client mode. Using `undo ntp-service multicast-client` command, you can disable the NTP multicast client mode.

By default, the multicast client service is disabled. *ip-address* defaults to 224.0.1.1.

Designate an interface on the local Ethernet Switch to receive NTP multicast messages and operate in multicast client mode. The local Ethernet Switch listens to the multicast from the server. When it receives the first multicast packet, it starts a brief client/server mode to switch messages with a remote server for estimating the network delay. Thereafter, the local Ethernet Switch enters multicast client mode and continues listening to the multicast and synchronizes the local clock according to the arrived multicast message.

**Example**

```
# Configure to receive NTP multicast packet via Vlan-Interface1 and the multicast group corresponding to these packets located at 224.0.1.1.
[Quidway] interface vlan-interface 1
[Quidway-Vlan-Interface1] ntp-service multicast-client 224.0.1.1
```

### 7.1.12 ntp-service multicast-server

**Syntax**

```
ntp-service multicast-server [ ip-address ] [ authentication-keyid keyid ] [ ttl ttl-number ] [ version number ]
undo ntp-service multicast-server [ ip-address ]
```

**View**

VLAN interface view

**Parameter**

*ip-address*: Specify a multicast IP address of Class D and default to 224.0.1.1.

*authentication-keyid*: Specify authentication key.

*keyid*: Key ID used in multicast, ranging from 0 to 4294967295.

*ttl*: Define the time to live of a multicast packet.

*ttl-number*: Specify the ttl of a multicast packet and range from 1 to 255.

*version*: Define NTP version number.
number: Specify NTP version number and range from 1 to 3.

Description

Using `ntp-service multicast-server` command, you can configure NTP multicast server mode, if no IP address is specified, switch automatically choose the 224.0.1.1 as the multicast IP address. Using `undo ntp-service multicast-server` command, you can disable NTP multicast server mode, if no IP address is specified, the switch will disable the configuration of the multicast IP address 224.0.1.1.

By default, the multicast service is disabled. IP address defaults to 224.0.1.1 and the version number defaults to 3.

Designate an interface on the local equipment to transmit NTP multicast packet. The local equipment operates in multicast-server mode and multicasts packets regularly to its clients.

Example

# Configure to transmit NTP multicast packets encrypted with Key 4 via Vlan-Interface1 at 224.0.1.1 and use NTP version 3.

```plaintext
[Quidway] interface vlan-interface 1
[Quidway-Vlan-Interface1] ntp-service multicast-server 224.0.1.1
authentication-keyid 4 version 3
```

7.1.13 ntp-service refclock-master

Syntax

```
ntp-service refclock-master [ ip-address ] [ stratum ]
undo ntp-service refclock-master [ ip-address ]
```

View

System view

Parameter

`ip-address`: Specify the reference clock IP address as 127.127.t.u. Here, t ranges from 0 to 37 and u ranges from 0 to 3.

`stratum`: Specify which stratum the local clock is located at and range from 1 to 15.

Description

Using `ntp-service refclock-master` command, you can configure an external reference clock or the local clock as an NTP master clock. Using `undo ntp-service refclock-master` command, you can cancel the NTP master clock settings.

By default, `ip-address` is not specified and `stratum` defaults to 1.
You can use this command to designate an NTP external reference clock or the local clock as an NTP master clock to provide synchronized time for other equipment. `ip-address` specifies the IP address of an external clock as 127.127.t.u. If no IP address is specified, the local clock is set as the NTP master clock by default. You can also specify the stratum of the NTP master clock.

**Example**

```
# Set the local clock as the NTP master clock to provide synchronized time for its peers and locate it at stratum 3.
[Quidway] ntp-service refclock-master 3
```

### 7.1.14 ntp-service reliable authentication-keyid

**Syntax**

```
ntp-service reliable authentication-keyid number
undo ntp-service reliable authentication-keyid number
```

**View**

System view

**Parameter**

`number`: Specify the key number, ranging from 1 to 4294967295.

**Description**

Using `ntp-service reliable authentication-keyid` command, you can configure the key as reliable. Using `undo ntp-service reliable authentication-keyid` command, you can cancel the current setting.

By default, no key is configured as reliable.

When you enable the authentication, you can use this command to configure one or more than one keys as reliable. In this case, a client will only get synchronized by a server whichever can provide a reliable key.

**Example**

```
# Enable NTP authentication, adopt MD5 encryption, and designate Key 37 BetterKey and configure it as reliable.
[Quidway] ntp-service authentication enable
[Quidway] ntp-service authentication-keyid 37 authentication-mode md5 BetterKey
[Quidway] ntp-service reliable authentication-keyid 37
```
7.1.15 ntp-service source-interface

Syntax

ntp-service source-interface { interface-name | interface-type interface-number }
undo ntp-service source-interface

View

System view

Parameter

interface-name: Specify an interface. The source IP address of the packets will be taken from the address of the interface.
interface-type: Specify the interface type and determine an interface with the interface-number parameter.
interface-number: Specify the interface number and determine an interface with the interface-type parameter.

Description

Using ntp-service source-interface command, you can designate an interface to transmit NTP message. Using undo ntp-service source-interface command, you can cancel the current setting.

The source address specifies where the packets are transmitted from.

You can use this command to designate an interface to transmit all the NTP packets and take the source address of these packets from its IP address. If you do not want any other interface to receive the acknowledgement packets, use this command to specify one interface to send all the NTP packets.

Example

# Configure all the outgoing NTP packets to use the IP address of Vlan-Interface1 as their source IP address.
[Quidway] ntp-service source-interface Vlan-Interface 1

7.1.16 ntp-service in-interface disable

Syntax

ntp-service in-interface disable
undo ntp-service in-interface disable

View

VLAN interface view
Parameter
None

Description
Using **ntp-service in-interface disable** command, you can disable an interface to receive NTP message. Using **undo ntp-service in-interface disable** command, you can enable an interface to receive NTP message.
By default, an interface is enabled to receive NTP message.

Example

```
# Disable Vlan-Interface1 to receive NTP message.
[Quidway] interface vlan-interface1
[Quidway-Vlan-Interface1] ntp-service in-interface disable
```

### 7.1.17 ntp-service unicast-peer

**Syntax**

```
ntp-service unicast-peer ip-address [ version number ] [ authentication-key keyid ] [ source-interface { interface-name | interface-type interface-number } ] [ priority ]
undo ntp-service unicast-peer ip-address
```

**View**

System view

**Parameter**

- **ip-address**: Specify the IP address of a remote server.
- **version**: Define NTP version number.
- **number**: NTP version number, ranging from 1 to 3.
- **authentication-keyid**: Define authentication key.
- **keyid**: Key ID used for transmitting messages to a remote server, ranging from 0 to 4294967295.
- **source-interface**: Specify the name of an interface.
- **interface-name**: Specify the interface name. When a local device sends an NTP message to a peer, the source IP address of the message is taken from the address of the interface.
- **interface-type**: Specify the interface type and determine an interface together with the **interface-number** parameter.
- **interface-number**: Specify the interface number and determine an interface together with the **interface-type** parameter.
priority: Designate a server as the first choice.

Description

Using `ntp-service unicast-peer` command, you can configure NTP peer mode. Using `undo ntp-service unicast-peer` command, you can cancel NTP peer mode.

By default, version number `number` defaults to 3, the authentication is disabled, and the local server is not the first choice.

This command sets the remote server at `ip-address` as a peer of the local equipment, which operates in symmetric active mode. `ip-address` specifies a host address other than an IP address of broadcast, multicast, or reference clock. By operating in this mode, a local device can synchronize and be synchronized by a remote server.

Example

```
# Configure the local equipment to synchronize or synchronized by a peer at 128.108.22.44. Set the NTP version to 3. The IP address of the NTP packets are taken from that of Vlan-Interface1.

[Quidway] ntp-service unicast-peer 131.108.22.33 version 3 source-interface Vlan-Interface 1
```

7.1.18 ntp-service unicast-server

Syntax

```
ntp-service unicast-server ip-address [ version number ] [ authentication-keyid keyid ] [ source-interface { interface-name | interface-type interface-number } ] [ priority ]
undo ntp-service unicast-server ip-address
```

View

System view

Parameter

- `ip-address`: Specify the IP address of a remote server.
- `version`: Define NTP version number.
- `number`: NTP version number, ranging from 1 to 3.
- `authentication-keyid`: Define authentication key.
- `keyid`: Key ID used for transmitting messages to a remote server, ranging from 0 to 4294967295.
- `source-interface`: Specify the name of an interface.
**Command Manual - System Management**  
**Quidway S3000-EI Series Ethernet Switches**  
**Chapter 7  NTP Configuration Commands**

*interface-name:* Specify the interface name. When a local device sends an NTP message to a peer, the source IP address of the message is taken from the address of the interface.

*interface-type:* Specify the interface type and determine an interface together with the *interface-number* parameter.

*interface-number:* Specify the interface number and determine an interface together with the *interface-type* parameter.

*priority:* Designate a server as the first choice.

**Description**

Using **ntp-service unicast-server** command, you can configure NTP server mode. Using **undo ntp-service unicast-server** command, you can disable NTP server mode.

By default, version number *number* defaults to 3, the authentication is disabled, and the local server is not the first choice.

The command announces to use the remote server at *ip-address* as the local time server. *ip-address* specifies a host address other than an IP address of broadcast, multicast, or reference clock. By operating in client mode, a local device can be synchronized by a remote server, but not synchronize any remote server.

**Example**

```
# Designate the server at 128.108.22.44 to synchronize the local device and use NTP version 3.

[Quidway] ntp-service unicast-server 128.108.22.44 version 3
```
Chapter 8  SSH Configuration Commands

8.1  SSH Configuration Commands

8.1.1  debugging rsa

Command

ddebugging rsa
undo debugging rsa

View

User view

Parameter

None

Description

Using the debugging rsa command, you can send the detailed information of RSA algorithm, including every process and packet structure, to the information center as debugging information. Using the undo debugging rsa command, you can disable debugging function.

By default, debugging function is disabled.

For the related commands, see rsa local-key-pair create, rsa local-key-pair destroy.

Example

# Enable RSA debugging.
<Quidway> debugging rsa

8.1.2  debugging ssh server

Command

ddebugging ssh server { all | vty index }
undo debugging ssh server { all | vty index }

View

User view
Parameter

**all**: All SSH channels

**index**: Debugged SSH channels. Optional values depend on the VTY number and they are 0~4.

Description

Using the `debugging ssh server` command, you can send the negotiation process defined in SSH1.5 protocol to the information center as debugging information and debug a single user interface. Using the `undo debugging ssh server` command, you can disable debugging function.

By default, debugging function is disabled.

For the related commands, see `ssh server authentication-retries`, `ssh server rekey-interval`, `ssh server timeout`.

Example

```bash
# Print debugging information in running SSH
<Quidway> debugging ssh server vty 0
00:23:20: SSH0: starting SSH control process
00:23:20: SSH0: sent protocol version id SSH-1.5-Quidway-1.25
00:23:20: SSH0: protocol version id is - SSH-1.5-1.2.26
00:23:20: SSH0: SSH_SMSG_PUBLIC_KEY msg
00:23:21: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:23:21: SSH: RSA decrypt started
00:23:21: SSH: RSA decrypt finished
00:23:21: SSH: RSA decrypt started
00:23:21: SSH: RSA decrypt finished
```

8.1.3 **display rsa local-key-pair public**

Command

`display rsa local-key-pair public`

View

Any view

Parameter

None
Description

Using the `display rsa local-key-pair public` command, you can display local key pair and public key of the server. If no key is generated, corresponding information will be prompted, for example, “RSA keys not found”.

For the related command, see `rsa local-key-pair create`.

Example

```bash
# Display local key pair and public key of the server.
<Quidway> display rsa local-key-pair public
% Key pair was generated at: 12:26:33 UTC 2002/4/4
Key name: rtvrp_Host
Usage: Encryption Key
Key Data:
30470240 AF7DB1D0 DA78944F 53B7B59B 40D425D0 DC9C57D2 A60916C2 1F165807
08B84DD5 5F4DB8E5 7A15B745 2D41D96C AC61D276 AA027E41 DD48DE64 696E0934
EB872805 02030100 01
% Key pair was generated at: 12:26:45 UTC 2002/4/4
Key name: rtvrp_Server
Usage: Encryption Key
Key Data:
30670260 C05280D9 BA0D56C8 7B577385 8634CDE7 83ABA9A2 3F36280E 25995487
4FF6AD7A 0E57871C 761E6D92 9914D8C5 CC577388 5B580B94 C2172C8F 36039EED
160A0478 651DED5A 9CCF1AAD D800AFF2 DF7FBEC4 A13ADA59 9E738319 AF366BB8
519D39F5 02030100 01
```

8.1.4 display rsa peer-public-key

Command

```bash
display rsa peer-public-key [ brief | name keyname ]
```

View

Any view

Parameter

- `brief`: Displays brief information of the remote public key.
- `keyname`: Specifies key name, a string including 0~32 characters.

Description

Using the `display rsa peer-public-key` command, you can display a designated RSA public key. All public keys will be displayed if no key is specified.

For the related command, see `rsa local-key-pair create`.

Huawei Technologies Proprietary
Example

```bash
# Display a designated RSA public key.
<Quidway> display rsa peer-public-key
Address  Bits   Name
  1023   abcd
  1024   hq
  1024   wn1
  1024   hq_all
<Quidway> display rsa peer-public-key name abcd
Key name:abcd
Key address:
  Data:
  30818602 8180739A 291ABDA7 04F5DF84C 42746319 91C164B0 DF178C55
  FA833591 C7D47D53 81D09CE8 2913D7ED F9C08511 D83CA4ED 2B30B809 808EB0D1
  F52D045D E40861B7 4A0E1355 23CCD74C AC61F8E5 8C452E2F 3F2DA0DC C48E3306
  367FE187 BDD94401 8B3B69F3 CBB0A573 202C16BB 2FC1ACF3 EC8F828D 55A36F1C
  DDC4BB45 504F0201 25

8.1.5 display ssh server

Command

display ssh server { session | status }

View

Any view

Parameter

**session**: Displays SSH sessions.
**status**: Displays SSH state information.

Description

Using the `display ssh server` command, you can display SSH state or session information.

For the related commands, see `ssh server authentication-retries`, `ssh server rekey-interval`, `ssh server timeout`.

Example

```bash
# Display SSH state and configuration parameters.
[Quidway] display ssh server status
SSH version : 1.5
SSH connection timeout : 60 seconds
```

Huawei Technologies Proprietary
SSH server key generating interval : 1 hours
SSH Authentication retries : 3 times

# Display SSH sessions.
[Quidway] display ssh server session

Connection    Version    Encryption    State                Username
VTY0          1.5         DES            Session started    Quidway
VTY3          1.5         DES            Session started    router

8.1.6 display ssh user-information

Command

display ssh user-information [ username ]

View

Any view

Parameter

username: Valid SSH user named defined by AAA

Description

Using the display ssh user-information command, you can display information of the user, including username, corresponding key, authentication type. If a username is specified, the system just gives its information.

For the related commands, see ssh user username assign rsa-key, ssh user username authentication-type.

Example

# Display SSH user information.
[Quidway] display ssh user-information

Username    authentication-type    user-public-key-name
Jin          rsa                   jin
hanqi1       password             816pub

8.1.7 peer-public-key end

Command

peer-public-key end

View

RSA public key view
Parameter

None

Description

Using the **peer-public-key end** command, you can finish editing peer public key and quit from RSA public key view to system view.

For the related commands, see **rsa peer-public-key**, **public-key-code end**.

Example

```
# Quit RSA public key view.
[Quidway] rsa peer-public-key quidway003
[Quidway-rsa-public-key] peer-public-key end
[Quidway]
```

### 8.1.8 protocol inbound

**Command**

```
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**

Using the **protocol inbound** command, you can configure the protocols supported by a designated user interface.

By default, the system supports both Telnet and SSH protocols.

If SSH protocol is enabled and specified for the user interface, but no local RSA key is configured, SSH cannot take effect yet till you log onto the system next time.

If SSH protocol is specified, to ensure a successful logon, you must configure the AAA authentication using the **authentication-mode scheme** command. The **protocol inbound ssh** configuration fails if you configure **authentication-mode password** and **authentication-mode none**.

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

# Disable Telnet on vty0 through vty4, only SSH available.
[Quidway] user-interface vty 0 4
[Quidway-ui-vty0-4] protocol inbound ssh

# Disable Telnet on vty0, only SSH available.
[Quidway] user-interface vty 0
[Quidway-ui-vty0] protocol inbound ssh

8.1.9 public-key-code begin

Command

public-key-code begin

View

RSA key code view

Parameter

None

Description

Using the `public-key-code begin` command, you can enter RSA key code view. Before using this command, you have to create a public key with the `rsa peer-public-key` command. In the RSA key code view, you can key in desired public key, which consists of hexadecimal characters, with blank space allowed between them, and is generated randomly by the client program supporting SSH.

For the related commands, see `rsa peer-public-key`, `public-key-code end`.

Example

# Enter RSA public key view and key in public key.
[Quidway] rsa peer-public-key quidway003
[Quidway-rsa-public-key] public-key-code begin
[Quidway-rsa-key-code] 3081B6028180739A291ABDA704F5D93DC8FDF84C427463
[Quidway-rsa-key-code] 1991C164B0DF178C55FA833591C7D47D5381D09CE82913
[Quidway-rsa-key-code] D7EDF9C08511DB3CA4ED2B30B809808EB0D1F52D045DE4
[Quidway-rsa-key-code] 0861B74A0E135523CDD74CAC61F8E58C452B2F32DA0DC
[Quidway-rsa-key-code] C48E3306367FE187DD944018B3B69F3CBB0A573202C16
[Quidway-rsa-key-code] BB2FC1ACF3EC8F828D55A36F1CDDC4BB45504F020125
[Quidway-rsa-key-code] public-key-code end
8.1.10  public-key-code end

Command
public-key-code end

View
RSA key code view

Parameter
None

Description
Using the public-key-code end command, you can save the configured public key and return to the RSA public key view from the RSA key code view.

This command terminates the edit process of public key and checks its validity before saving. If the public key contains invalid characters or violates coding rules, corresponding information will be prompted and the current configuration fails. If you have configured valid public key, the system will store it into the public key table.

For the related commands, see rsa peer-public-key, public-key-code begin.

Example

# Exit the RSA key code view and save the configuration.
[Quidway-rsa-key-code] public-key-code end
[Quidway-rsa-public-key]

8.1.11  rsa local-key-pair create

Command
rsa local-key-pair create

View
System view

Parameter
None

Description
Using the rsa local-key-pair create command, you can create local RSA host key pair and server key pair.

If you have configured RSA key, the system gives an alarm after using this command and prompts that the existing one will be replaced. The key naming format is switch
name plus server and switch name plus host, for example, Quidway_host and Quidway_server. The configuration result of this command will not be stored in the configuration file.

The system prompts you to key in bit range, for which, the server key pair must be at least 128 bits longer than the host key pair. The maximum bit range of both key pairs is 2048 bits and the minimum is 512. If there have been key pairs, the system will prompts you to decide whether to modify them.

For a successful SSH logon, you must configure and generate the local RSA key pairs. To generate local key pairs, you just need to execute the command once, with no further action required even after the system is rebooted.

For the related command, see rsa local-key-pair destroy.

Example

# Create local host key pair and server key pair.
[Quidway] rsa local-key-pair create
The key name will be: Quidway_Host
% You already have RSA keys defined for Quidway_Host
% Do you really want to replace them? [yes/no]:y
Choose the size of the key modulus in the range of 512 to 2048 for your Keys.
NOTES: If the key modulus is greater than 512,
    It will take a few minutes.
How many bits in the modulus [512]:512
Generating keys...
    ..................+++++++^
    .........................+++++++^
    ....................................+++++++^

[Quidway]

8.1.12 rsa local-key-pair destroy

Command

rsa local-key-pair destroy

View

System view

Parameter

None
### Description

Using the **rsa local-key-pair destroy** command, you can remove all RSA key pairs at the server, including Host key pair and Server key pair.

Acknowledgement information will be promoted before the system clears all RSA key pairs. This command is just a one-time instruction, so the result will not be stored in the configuration file.

For the related commands, see **rsa local-key-pair create**.

### Example

```
# Remove all key pairs at the server.
[Quidway] rsa local-key-pair destroy
% The name for the keys which will be destroyed is Quidway_Host.
% Confirm to destroy these keys? [yes/no]:y
[Quidway]
```

### 8.1.13 rsa peer-public-key

#### Command

**rsa peer-public-key** *key-name*

#### View

System view

#### Parameter

*key-name*: Public key name

#### Description

Using the **rsa peer-public-key** command, you can enter the RSA public key view.

When using this command together with the **public-key-code begin** command, you can configure the public key at the client, which is generated randomly by the client program supporting SSH1.5.

For the related commands, see **public-key-code begin**, **public-key-code end**.

#### Example

```
# Enter the RSA public key view.
[Quidway] rsa peer-public-key quidway002
[Quidway-rsa-public]
```
8.1.14  ssh server authentication-retries

Command

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

Using the ssh server authentication-retries command, you can define SSH authentication retry times value, which takes effect at next logon. Using the undo ssh server authentication-retries command, you can restore the default retry value.

By default, it is 3.

For the related command, see display ssh server.

Example

# Define the authentication retry times value as 4.
[Quidway] ssh server authentication-retries 4

8.1.15  ssh server rekey-interval

Command

ssh server rekey-interval hours
undo ssh server rekey-interval

View

System view

Parameter

hours: Defines key update interval, in the range of 1~24 hours.

Description

Using the ssh server rekey-interval command, you can define update interval of server key pair. Using the undo ssh server rekey-interval command, you can cancel the current setting.

By default, system doesn’t update the server key.
For the related commands, see `display ssh server`.

Example

```
# Define update interval of server key pair as 3 hours.
[Quidway] ssh server rekey-interval 3
[Quidway]
```

### 8.1.16 ssh server timeout

**Command**

```
ssh server timeout seconds
undo ssh server timeout
```

**View**

System view

**Parameter**

`seconds`: Defines registration timeout value, in the range of 1~120 seconds.

**Description**

Using the `ssh server timeout` command, you can define timeout value for SSH registration authentication, which takes effect at next logon. Using the `undo ssh server timeout` command, you can restore the default value.

By default, the timeout value is 60 seconds.

For the related commands, see `display ssh server`.

Example

```
# Define the registration timeout value as 80 seconds.
[Quidway] ssh server timeout 80
```

### 8.1.17 ssh user assign rsa-key

**Command**

```
ssh user username assign rsa-key keyname
undo ssh user username assign rsa-key
```

**View**

System view
Parameter

`keyname`: Configures client public key, consisting of 1~32 characters.

`username`: Valid local user name or user name defined by remote RADIUS system.

Description

Using the `ssh user username assign rsa-key` command, you can associate an existing public key with a designated user. Using the `undo ssh user username assign rsa-key` command, you can 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 newly configured users take effect at the next logon.

For the related command, see `display ssh user-information`.

Example

```
# Associate the key 1 with the zhangsan.
[Quidway] ssh user zhangsan assign rsa-key key1
[Quidway]
```

8.1.18 ssh user username authentication-type

Command

```
ssh user username authentication-type { all | password | rsa }
undo ssh user username authentication-type
```

View

System view

Parameter

`username`: Valid local user name or user name defined by remote RADIUS system.

`all`: Specifies authentication type as password and RSA.

`password`: Specifies authentication type as password.

`rsa`: Specifies authentication type as RSA.

Description

Using the `ssh user username authentication-type` command, you can define authentication type for a designated user. Using the `undo ssh user username authentication-type` command, you can restore the default mode in which logon fails.
By default, user can't logon the switch through SSH or TELNET, so you have to specify authentication type for a new user. The new configuration takes effects at the next logon.

For the related commands, see `display ssh user-information`.

**Example**

```
# Specify zhangsan's authentication type as password.
[Quidway] ssh user zhangsan authentication-type password
[Quidway]
```
Table of Contents

Chapter 1 Remote Power-feeding Configuration Commands ........................................... 1-1
  1.1 Remote Power-feeding Configuration Commands ...................................................... 1-1
       1.1.1 display poe interface ...................................................................................... 1-1
       1.1.2 display poe interface power .......................................................................... 1-2
       1.1.3 display poe powersupply ................................................................................ 1-3
       1.1.4 poe disable ..................................................................................................... 1-3
       1.1.5 poe legacy disable ......................................................................................... 1-4
       1.1.6 poe max-power............................................................................................... 1-5
       1.1.7 poe mode ........................................................................................................ 1-5
       1.1.8 poe power-management .................................................................................. 1-6
       1.1.9 poe priority ..................................................................................................... 1-7
       1.1.10 poe update ...................................................................................................... 1-7
       1.1.11 reset poe-configuration ............................................................................... 1-8
Chapter 1  Remote Power-feeding Configuration Commands

1.1  Remote Power-feeding Configuration Commands

1.1.1  display poe interface

Syntax

display poe interface { interface-name | interface-type interface-num | all }

View

Any view

Parameter

interface-name | interface-type interface-num: Port of the switch, for detailed description, please refer to Command Manual – Port.

all: view the remote power-feeding status of all ports.

Description

Using the display poe interface command, you can view the remote power-feeding status of specified port or all ports.

Example

# Display the remote power-feeding status of Ethernet0/1.
<Quidway> display poe interface ethernet0/1
Port power enabled :enable
Port power ON/OFF :off
Port power status :pse normal
Port power mode :signal
Port PD class :0
port power priority :low
Port max power :10000 mW
Port power :0 mW
Port Average power :0 mw
Port Peak power :0 mw
Port current :0 mA
Port voltage :2 V
1.1.2 display poe interface power

Syntax

display poe interface power { interface-name | interface-type interface-num | all }

View

Any view

Parameter

interface-name | interface-type interface-num: Port of the switch, for detailed description, please refer to Command Manual – Port.

all: view the power of all ports.

Description

Using the display poe interface power command, you can view the power of specified port or all ports.

Example

# Display the power of all ports.
<Quidway> display poe interface power all
Ethernet0/1 current power : 0 mw
Ethernet0/2 current power : 0 mw
Ethernet0/3 current power : 0 mw
Ethernet0/4 current power : 0 mw
Ethernet0/5 current power : 0 mw
Ethernet0/6 current power : 0 mw
Ethernet0/7 current power : 0 mw
Ethernet0/8 current power : 0 mw
Ethernet0/9 current power : 0 mw
Ethernet0/10 current power : 0 mw
Ethernet0/11 current power : 0 mw
Ethernet0/12 current power : 0 mw
Ethernet0/13 current power : 0 mw
Ethernet0/14 current power : 0 mw
Ethernet0/15 current power : 0 mw
Ethernet0/16 current power : 0 mw
Ethernet0/17 current power : 0 mw
Ethernet0/18 current power : 0 mw
Ethernet0/19 current power : 0 mw
Ethernet0/20 current power : 0 mw
Ethernet0/21 current power : 0 mw
1.1.3 display poe powersupply

Syntax

display poe powersupply

View

Any view

Parameter

None.

Description

Using the `display poe powersupply` command, you can view the PoE parameters of PSE power supply device.

Example

```
# Display the PoE parameters of PSE power supply device.
<Quidway> display poe powersupply
PSE ID : 0
PSE Legacy Detection : disable
PSE PowerManagement : manual
PSE Total Power : 200000 mW
PSE Available Power : 196400 mW
PSE Average Power : 3600 mW
PSE Peak Power : 3600 mW
PSE Software Version : 100
PSE Hardware Version : 0
PSE CPLD Version : 1
```
Parameter

None

Description

Using the `poe disable` command, you can disable remote power-feeding on a port. Using the `undo poe disable` command, you can restore the default value.

By default, a port is enabled to perform remote power-feeding.

Example

```
# Disable Ethernet0/1 to perform remote power-feeding.
[Quidway-Ethernet0/1] poe disable
```

1.1.5 `poe legacy disable`

Syntax

```
poe legacy disable
undo poe legacy disable
```

View

System view

Parameter

None

Description

Using the `poe legacy disable` command, you can disable the switch to perform compatibility detection of PDs connected to it. Using the `undo poe legacy disable` command, you can enable switch to perform compatibility detection of its connected PDs.

By default, the switch is enabled to perform compatibility detection of its connected PDs.

The compatibility detection of PDs enables an S3026C-PWR to detect those PDs not complying with 802.3af standard and supply power to them. This process will reduce system rate and the system performance. If all PDs are complying with 802.3af standard, you are recommended to disable this function.

Example

```
# Enable an S3026C-PWR to perform compatibility detection of PDs connected to it.
[Quidway] undo poe legacy disable
```
1.1.6  poe max-power

Syntax

```
poe max-power max-power
undo poe max-power
```

View

Ethernet port view

Parameter

```
max-power: The maximum power supplied by a port, ranging from 100 to 15400 milliwatt.
```

Description

Using the `poe max-power` command, you can configure the maximum power supplied by a port.

By default, a port supplies power under a maximum of 15400 milliwatt.

You can adjust this maximum according to the actual power of the PDs.

Example

```
# Configure the current port Ethernet0/1 to supply power under a maximum of 1000 milliwatt.
[Quidway-Ethernet0/1] poe max-power 1000
```

1.1.7  poe mode

Syntax

```
poe mode { signal | spare }
undo poe mode
```

View

Ethernet port view

Parameter

```
signal: The port supplies power through signal lines.
spare: The port supplies power through spare lines.
```

Description

Using the `poe mode` command, you can configure the power supply mode of the current port. Using the `undo poe mode` command, you can restore the default value.
By default, a port supplies power through signal lines.

Example

```python
# Configure the current port Ethernet0/1 to supply power through signal lines.
[Quidway-Ethernet0/1] poe mode signal
```

1.1.8 poe power-management

Syntax

```python
poe power-management { auto | manual }
undo poe power-management
```

View

System view

Parameter

- `auto`: auto power management mode.
- `manual`: manual power management mode.

Description

Using the `poe power-management` command, you can configure the power management mode. Using the `undo poe power-management` command, you can restore the default value.

By default, the power management mode is manual mode.

This command is used with poe priority of the switch port together. It will be effective when power supply reaches full load.

- `auto`: when power supply reaches full load, the switch prefers to supply power to those PDs connected to a port of a "critical" priority rather than supply power to PDs connected to a port of a "high" or "low" priority. For example, port A is configured with a priority of "critical" and is connected to a new PD when the S3026C-PWR supplies power to the full, then the S3026C-PWR will automatically stop supplying power to any PD connected to a port of a "low" priority and give the chance to that new PD of port A.

- `manual`: when power supply reaches full load, the switch only gives prompt and doesn’t supply power to the new one if a new PD is connected to the switch. For example, port A is configured with a priority of "critical" and is connected to a new PD when the S3026C-PWR supplies power to the full, then the S3026C-PWR only gives prompt that a new PD is connected and doesn’t supply power to it.

Example

```python
# Configure the power management mode in auto mode.
```

Huawei Technologies Proprietary
1.1.9 poe priority

Syntax

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

View

    Ethernet port view

Parameter

    critical: The power supply priority of the port is critical.
    high: The power supply priority of the port is high.
    low: The power supply priority of the port is low.

Description

Using the poe priority command, you can configure the power supply priority of the current port. Using the undo poe priority command, you can restore the default value. By default, the power supply priority of the current port is low. This command is used with power management of switch together. It will be effective when power supply reaches full load. Please refer to the poe power-management command.

Example

    # Configure Ethernet0/1 with a power supply priority of high.
    [Quidway-Ethernet0/1] poe priority high

1.1.10 poe update

Syntax

    poe update file-url

View

    System view

Parameter

    file-url: the uniform resource locater of PoE daughter-card application.
Description

Using the `poe update` command, you can upgrade PoE daughter-card. PoE function relies on the PoE daughter-card inside the switch. User can use this command to upgrade the application of PoE daughter-card, and the switch service is not interruptive during this process. The extent name of the application file should be "bin".

Example

```bash
# Use file "flash:/new.bin" to upgrade the PoE daughter-card.
[Quidway] poe update flash:/new.bin
```

1.1.11 `reset poe-configuration`

Syntax

`reset poe-configuration`

View

User view

Parameter

None

Description

Using the `reset poe-configuration` command, you can restore the default PoE configuration on the current switch.

Example

```bash
# Restore the default PoE configuration on the current switch.
<Quidway> reset poe-configuration
This will delete the poe configuration in the flash memory.
The poe configurations will be erased to reconfigure.
Default poe configurations will be in effect now !
Are you sure?[Y/N]y
POE configuration is default!
```
Table of Contents

Appendix A Command Index .............................................................................................................A-1
Appendix A  Command Index

The command index includes all the commands in the Command Manual, which are arranged alphabetically.

A  B  C  D  E  F  G  H  I  J  K  L  M  N  O  P  Q  R  S  T  U  V  W  X  Y  Z

A

access-limit                    Security  2-1
accounting optional            Security  2-20
accounting-on enable           Security  2-18
acl                            QoS/ACL  1-1
acl                            QoS/ACL  3-1
active region-configuration    STP    1-1
add-member                     Integrated Management  2-14
administrator-address          Integrated Management  2-15
am enable                      Network Protocol  5-1
am isolate                     Network Protocol  5-1
am user-bind                   Network Protocol  5-2
arp check enable               Network Protocol  1-1
arp static                     Network Protocol  1-1
arp timer aging                Network Protocol  1-2
ascii                          System Management  1-18
attribute                      Security  2-2
authentication-mode            Getting Started  1-1
auto-build                     Integrated Management  2-15
auto-execute command           Getting Started  1-1

B

binary                        System Management  1-18
boot boot-loader               System Management  3-1
boot bootrom System Management 3-1
broadcast-suppression Port 1-1
build Integrated Management 2-16
bye System Management 1-19

C

cd System Management 1-1
cd System Management 1-19
cdup System Management 1-20
check region-configuration STP 1-1
clock datetime System Management 4-1
clock summer-time System Management 4-1
clock timezone System Management 4-3
close System Management 1-20
cluster Integrated Management 2-17
cluster enable Integrated Management 2-17
cluster switch-to Integrated Management 2-18
cluster-mac Integrated Management 3-1
cluster-mac syn-interval Integrated Management 3-1
command-privilege level Getting Started 1-2
copy System Management 1-1
cut connection Security 2-3

D
databits Getting Started 1-3
data-flow-format Security 2-20
debugging System Management 1-21
debugging System Management 4-13
debugging arp packet Network Protocol 1-3
debugging bootp client Network Protocol 4-1
debugging dhcp client Network Protocol 3-1
<table>
<thead>
<tr>
<th>Command</th>
<th>Category</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>debugging gmrp</td>
<td>Multicast</td>
<td>1-1</td>
</tr>
<tr>
<td>debugging ntp-service</td>
<td>System Management</td>
<td>7-1</td>
</tr>
<tr>
<td>debugging rsa</td>
<td>System Management</td>
<td>8-1</td>
</tr>
<tr>
<td>debugging ssh server</td>
<td>System Management</td>
<td>8-1</td>
</tr>
<tr>
<td>delete</td>
<td>System Management</td>
<td>1-2</td>
</tr>
<tr>
<td>delete</td>
<td>System Management</td>
<td>1-21</td>
</tr>
<tr>
<td>delete-member</td>
<td>Integrated Management</td>
<td>2-19</td>
</tr>
<tr>
<td>description</td>
<td>Getting Started</td>
<td>2-1</td>
</tr>
<tr>
<td>description</td>
<td>Port</td>
<td>1-1</td>
</tr>
<tr>
<td>description</td>
<td>VLAN</td>
<td>1-1</td>
</tr>
<tr>
<td>dhcp-snooping</td>
<td>Network Protocol</td>
<td>2-1</td>
</tr>
<tr>
<td>dhcp-snooping trust</td>
<td>Network Protocol</td>
<td>2-1</td>
</tr>
<tr>
<td>dir</td>
<td>System Management</td>
<td>1-3</td>
</tr>
<tr>
<td>dir</td>
<td>System Management</td>
<td>1-22</td>
</tr>
<tr>
<td>disconnect</td>
<td>System Management</td>
<td>1-22</td>
</tr>
<tr>
<td>display acl config</td>
<td>QoS/ACL</td>
<td>1-2</td>
</tr>
<tr>
<td>display acl running-packet-filter all</td>
<td>QoS/ACL</td>
<td>1-3</td>
</tr>
<tr>
<td>display am</td>
<td>Network Protocol</td>
<td>5-3</td>
</tr>
<tr>
<td>display am user-bind</td>
<td>Network Protocol</td>
<td>5-4</td>
</tr>
<tr>
<td>display arp</td>
<td>Network Protocol</td>
<td>1-4</td>
</tr>
<tr>
<td>display arp timer aging</td>
<td>Network Protocol</td>
<td>1-5</td>
</tr>
<tr>
<td>display boot-loader</td>
<td>System Management</td>
<td>3-2</td>
</tr>
<tr>
<td>display bootp client</td>
<td>Network Protocol</td>
<td>4-1</td>
</tr>
<tr>
<td>display channel</td>
<td>System Management</td>
<td>4-19</td>
</tr>
<tr>
<td>display clock</td>
<td>System Management</td>
<td>4-4</td>
</tr>
<tr>
<td>display cluster</td>
<td>Integrated Management</td>
<td>2-20</td>
</tr>
<tr>
<td>display cluster candidates</td>
<td>Integrated Management</td>
<td>2-22</td>
</tr>
<tr>
<td>display cluster members</td>
<td>Integrated Management</td>
<td>2-23</td>
</tr>
<tr>
<td>display connection</td>
<td>Security</td>
<td>2-4</td>
</tr>
<tr>
<td>display cpu</td>
<td>System Management</td>
<td>3-2</td>
</tr>
<tr>
<td>display current-configuration</td>
<td>System Management</td>
<td>4-5</td>
</tr>
<tr>
<td>Command</td>
<td>Category</td>
<td>Page</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------</td>
<td>------</td>
</tr>
<tr>
<td>display debug</td>
<td>System Management</td>
<td>4-9</td>
</tr>
<tr>
<td>display debug habp</td>
<td>Security</td>
<td>3-1</td>
</tr>
<tr>
<td>display device</td>
<td>System Management</td>
<td>3-3</td>
</tr>
<tr>
<td>display dhcp client</td>
<td>Network Protocol</td>
<td>3-1</td>
</tr>
<tr>
<td>display dhcp-snooping</td>
<td>Network Protocol</td>
<td>2-2</td>
</tr>
<tr>
<td>display dhcp-snooping count</td>
<td>Network Protocol</td>
<td>2-3</td>
</tr>
<tr>
<td>display dhcp-snooping trust</td>
<td>Network Protocol</td>
<td>2-3</td>
</tr>
<tr>
<td>display diagnostic-information</td>
<td>System Management</td>
<td>4-14</td>
</tr>
<tr>
<td>display domain</td>
<td>Security</td>
<td>2-5</td>
</tr>
<tr>
<td>display dot1x</td>
<td>Security</td>
<td>1-1</td>
</tr>
<tr>
<td>display environment</td>
<td>System Management</td>
<td>3-4</td>
</tr>
<tr>
<td>display fan</td>
<td>System Management</td>
<td>3-5</td>
</tr>
<tr>
<td>display fib</td>
<td>Network Protocol</td>
<td>6-1</td>
</tr>
<tr>
<td>display ftp-server</td>
<td>System Management</td>
<td>1-13</td>
</tr>
<tr>
<td>display ftp-user</td>
<td>System Management</td>
<td>1-14</td>
</tr>
<tr>
<td>display garp statistics</td>
<td>VLAN</td>
<td>3-1</td>
</tr>
<tr>
<td>display garp timer</td>
<td>VLAN</td>
<td>3-2</td>
</tr>
<tr>
<td>display gmrp statistics</td>
<td>Multicast</td>
<td>1-1</td>
</tr>
<tr>
<td>display gmrp status</td>
<td>Multicast</td>
<td>1-2</td>
</tr>
<tr>
<td>display gvrp statistics</td>
<td>VLAN</td>
<td>3-5</td>
</tr>
<tr>
<td>display gvrp status</td>
<td>VLAN</td>
<td>3-6</td>
</tr>
<tr>
<td>display habp</td>
<td>Security</td>
<td>3-1</td>
</tr>
<tr>
<td>display habp table</td>
<td>Security</td>
<td>3-2</td>
</tr>
<tr>
<td>display habp traffic</td>
<td>Security</td>
<td>3-2</td>
</tr>
<tr>
<td>display history-command</td>
<td>Getting Started</td>
<td>1-4</td>
</tr>
<tr>
<td>display icmp statistics</td>
<td>Network Protocol</td>
<td>6-2</td>
</tr>
<tr>
<td>display igmp-snooping configuration</td>
<td>Multicast</td>
<td>2-1</td>
</tr>
<tr>
<td>display igmp-snooping group</td>
<td>Multicast</td>
<td>2-2</td>
</tr>
<tr>
<td>display igmp-snooping statistics</td>
<td>Multicast</td>
<td>2-3</td>
</tr>
<tr>
<td>display info-center</td>
<td>System Management</td>
<td>4-19</td>
</tr>
<tr>
<td>display interface</td>
<td>Port</td>
<td>1-2</td>
</tr>
<tr>
<td>display interface vlan-interface</td>
<td>Getting Started</td>
<td>2-1</td>
</tr>
<tr>
<td>display ip host</td>
<td>Getting Started</td>
<td>2-2</td>
</tr>
<tr>
<td>display ip interface vlan-interface</td>
<td>Getting Started</td>
<td>2-3</td>
</tr>
</tbody>
</table>
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
display ip socket
display ip statistics
display isolate-user-vlan
display link-aggregation
display local-server statistics
display local-user
display loopback-detection
display mac-address
display mac-address aging-time
display memory
display multicast-source-deny
display ndp
display ntdp
display ntdp device-list
display ntp-service sessions
display ntp-service status
display ntp-service trace
display poe interface
display poe interface power
display poe powersupply
display port
<table>
<thead>
<tr>
<th>Command</th>
<th>Category</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>display power</td>
<td>System Management</td>
<td>3-6</td>
</tr>
<tr>
<td>display qos cos-local-precedence-map</td>
<td>QoS/ACL</td>
<td>2-1</td>
</tr>
<tr>
<td>display qos-global all</td>
<td>QoS/ACL</td>
<td>2-1</td>
</tr>
<tr>
<td>display qos-global mirrored-to</td>
<td>QoS/ACL</td>
<td>2-3</td>
</tr>
<tr>
<td>display qos-global traffic-priority</td>
<td>QoS/ACL</td>
<td>2-4</td>
</tr>
<tr>
<td>display qos-global traffic-redirect</td>
<td>QoS/ACL</td>
<td>2-5</td>
</tr>
<tr>
<td>display qos-global traffic-statistic</td>
<td>QoS/ACL</td>
<td>2-6</td>
</tr>
<tr>
<td>display qos-interface all</td>
<td>QoS/ACL</td>
<td>2-7</td>
</tr>
<tr>
<td>display qos-interface line-rate</td>
<td>QoS/ACL</td>
<td>2-9</td>
</tr>
<tr>
<td>display qos-interface traffic-limit</td>
<td>QoS/ACL</td>
<td>2-9</td>
</tr>
<tr>
<td>display queue-scheduler</td>
<td>QoS/ACL</td>
<td>2-11</td>
</tr>
<tr>
<td>display radius</td>
<td>Security</td>
<td>2-22</td>
</tr>
<tr>
<td>display radius statistics</td>
<td>Security</td>
<td>2-23</td>
</tr>
<tr>
<td>display rmon alarm</td>
<td>System Management</td>
<td>6-1</td>
</tr>
<tr>
<td>display rmon event</td>
<td>System Management</td>
<td>6-2</td>
</tr>
<tr>
<td>display rmon eventlog</td>
<td>System Management</td>
<td>6-3</td>
</tr>
<tr>
<td>display rmon history</td>
<td>System Management</td>
<td>6-4</td>
</tr>
<tr>
<td>display rmon prialarm</td>
<td>System Management</td>
<td>6-5</td>
</tr>
<tr>
<td>display rmon statistics</td>
<td>System Management</td>
<td>6-7</td>
</tr>
<tr>
<td>display rsa local-key-pair public</td>
<td>System Management</td>
<td>8-2</td>
</tr>
<tr>
<td>display rsa peer-public-key</td>
<td>System Management</td>
<td>8-3</td>
</tr>
<tr>
<td>display saved-configuration</td>
<td>System Management</td>
<td>4-9</td>
</tr>
<tr>
<td>display snmp-agent</td>
<td>System Management</td>
<td>5-1</td>
</tr>
<tr>
<td>display snmp-agent community</td>
<td>System Management</td>
<td>5-1</td>
</tr>
<tr>
<td>display snmp-agent group</td>
<td>System Management</td>
<td>5-2</td>
</tr>
<tr>
<td>display snmp-agent mib-view</td>
<td>System Management</td>
<td>5-3</td>
</tr>
<tr>
<td>display snmp-agent statistics</td>
<td>System Management</td>
<td>5-4</td>
</tr>
<tr>
<td>display snmp-agent sys-info contact</td>
<td>System Management</td>
<td>5-5</td>
</tr>
<tr>
<td>display snmp-agent sys-info location</td>
<td>System Management</td>
<td>5-6</td>
</tr>
<tr>
<td>display snmp-agent sys-info version</td>
<td>System Management</td>
<td>5-6</td>
</tr>
<tr>
<td>display snmp-agent usm-user</td>
<td>System Management</td>
<td>5-7</td>
</tr>
<tr>
<td>display ssh server</td>
<td>System Management</td>
<td>8-4</td>
</tr>
<tr>
<td>display ssh user-information</td>
<td>System Management</td>
<td>8-5</td>
</tr>
<tr>
<td>Command</td>
<td>Category</td>
<td>Page</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------</td>
<td>------</td>
</tr>
<tr>
<td>display stacking</td>
<td>Integrated</td>
<td>1-1</td>
</tr>
<tr>
<td>display stop-accounting-buffer</td>
<td>Security</td>
<td>2-24</td>
</tr>
<tr>
<td>display stp</td>
<td>STP</td>
<td>1-3</td>
</tr>
<tr>
<td>display stp region-configuration</td>
<td>STP</td>
<td>1-5</td>
</tr>
<tr>
<td>display tcp statistics</td>
<td>Network Protocol</td>
<td>6-6</td>
</tr>
<tr>
<td>display tcp status</td>
<td>Network Protocol</td>
<td>6-8</td>
</tr>
<tr>
<td>display time-range</td>
<td>QoS/ACL</td>
<td>1-4</td>
</tr>
<tr>
<td>display user-interface</td>
<td>Getting Started</td>
<td>1-5</td>
</tr>
<tr>
<td>display users</td>
<td>Getting Started</td>
<td>1-6</td>
</tr>
<tr>
<td>display users</td>
<td>System Management</td>
<td>4-12</td>
</tr>
<tr>
<td>display version</td>
<td>System Management</td>
<td>4-12</td>
</tr>
<tr>
<td>display vlan</td>
<td>VLAN</td>
<td>1-1</td>
</tr>
<tr>
<td>display voice vlan oui</td>
<td>VLAN</td>
<td>4-1</td>
</tr>
<tr>
<td>display voice vlan status</td>
<td>VLAN</td>
<td>4-1</td>
</tr>
<tr>
<td>domain</td>
<td>Security</td>
<td>2-8</td>
</tr>
<tr>
<td>dot1x</td>
<td>Security</td>
<td>1-2</td>
</tr>
<tr>
<td>dot1x authentication-method</td>
<td>Security</td>
<td>1-3</td>
</tr>
<tr>
<td>dot1x dhcp-launch</td>
<td>Security</td>
<td>1-4</td>
</tr>
<tr>
<td>dot1x dynamic-binding-user enable</td>
<td>Security</td>
<td>1-5</td>
</tr>
<tr>
<td>dot1x guest-vlan</td>
<td>Security</td>
<td>1-6</td>
</tr>
<tr>
<td>dot1x max-user</td>
<td>Security</td>
<td>1-7</td>
</tr>
<tr>
<td>dot1x port-control</td>
<td>Security</td>
<td>1-8</td>
</tr>
<tr>
<td>dot1x port-method</td>
<td>Security</td>
<td>1-9</td>
</tr>
<tr>
<td>dot1x quiet-period</td>
<td>Security</td>
<td>1-10</td>
</tr>
<tr>
<td>dot1x re-authenticate</td>
<td>Security</td>
<td>1-11</td>
</tr>
<tr>
<td>dot1x retry</td>
<td>Security</td>
<td>1-12</td>
</tr>
<tr>
<td>dot1x retry-version-max</td>
<td>Security</td>
<td>1-13</td>
</tr>
<tr>
<td>dot1x supp-proxy-check</td>
<td>Security</td>
<td>1-13</td>
</tr>
<tr>
<td>dot1x timer</td>
<td>Security</td>
<td>1-15</td>
</tr>
<tr>
<td>dot1x version-check</td>
<td>Security</td>
<td>1-16</td>
</tr>
<tr>
<td>duplex</td>
<td>Port</td>
<td>1-7</td>
</tr>
<tr>
<td>Command</td>
<td>Category</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------</td>
<td>------</td>
</tr>
<tr>
<td>file prompt</td>
<td>System Management</td>
<td>1-4</td>
</tr>
<tr>
<td>flow-constrain</td>
<td>Port</td>
<td>1-7</td>
</tr>
<tr>
<td>flow-constrain method</td>
<td>Port</td>
<td>1-8</td>
</tr>
<tr>
<td>flow-control</td>
<td>Getting Started</td>
<td>1-7</td>
</tr>
<tr>
<td>flow-control</td>
<td>Port</td>
<td>1-9</td>
</tr>
<tr>
<td>flow-interval</td>
<td>Port</td>
<td>1-9</td>
</tr>
<tr>
<td>format</td>
<td>System Management</td>
<td>1-5</td>
</tr>
<tr>
<td>free user-interface</td>
<td>Getting Started</td>
<td>1-7</td>
</tr>
<tr>
<td>ftp</td>
<td>System Management</td>
<td>1-23</td>
</tr>
<tr>
<td>ftp server</td>
<td>System Management</td>
<td>1-14</td>
</tr>
<tr>
<td>ftp timeout</td>
<td>System Management</td>
<td>1-15</td>
</tr>
<tr>
<td>ftp-server</td>
<td>Integrated Management</td>
<td>2-25</td>
</tr>
<tr>
<td>garp timer</td>
<td>VLAN</td>
<td>3-2</td>
</tr>
<tr>
<td>garp timer leaveall</td>
<td>VLAN</td>
<td>3-3</td>
</tr>
<tr>
<td>get</td>
<td>System Management</td>
<td>1-23</td>
</tr>
<tr>
<td>gmrp</td>
<td>Multicast</td>
<td>1-3</td>
</tr>
<tr>
<td>gratuitous-arp-learning enable</td>
<td>Network Protocol</td>
<td>1-6</td>
</tr>
<tr>
<td>gvrp</td>
<td>VLAN</td>
<td>3-6</td>
</tr>
<tr>
<td>gvrp registration</td>
<td>VLAN</td>
<td>3-7</td>
</tr>
<tr>
<td>habp enable</td>
<td>Security</td>
<td>3-3</td>
</tr>
<tr>
<td>habp server vlan</td>
<td>Security</td>
<td>3-4</td>
</tr>
<tr>
<td>habp timer</td>
<td>Security</td>
<td>3-4</td>
</tr>
<tr>
<td>header</td>
<td>Getting Started</td>
<td>1-8</td>
</tr>
<tr>
<td>history-command max-size</td>
<td>Getting Started</td>
<td>1-10</td>
</tr>
<tr>
<td>holdtime</td>
<td>Integrated Management</td>
<td>2-26</td>
</tr>
</tbody>
</table>
idle-cut  Security  2-9
idle-timeout  Getting Started  1-10
igmp-snooping  Multicast  2-4
igmp-snooping fast-leave  Multicast  2-5
igmp-snooping group-limit  Multicast  2-5
igmp-snooping group-policy  Multicast  2-6
igmp-snooping host-aging-time  Multicast  2-8
igmp-snooping max-response-time  Multicast  2-8
igmp-snooping router-aging-time  Multicast  2-9
info-center channel name  System Management  4-21
info-center console channel  System Management  4-21
info-center enable  System Management  4-22
info-center logbuffer  System Management  4-23
info-center loghost  System Management  4-23
info-center loghost source  System Management  4-24
info-center monitor channel  System Management  4-25
info-center snmp channel  System Management  4-26
info-center source  System Management  4-26
info-center switch-on  System Management  4-28
info-center timestamp  System Management  4-29
info-center trapbuffer  System Management  4-30
instance  STP  1-6
interface  Port  1-10
interface vlan-interface  Getting Started  2-17
ip address  Getting Started  2-18
ip address bootp-alloc  Network Protocol  4-2
ip address dhcp-alloc  Network Protocol  3-2
ip host  Getting Started  2-18
ip http acl  QoS/ACL  3-1
ip route-static  Getting Started  2-19
ip route-static default-preference  Getting Started  2-20
ip-pool  Integrated Management  2-27
isolate-user-vlan  VLAN  2-2
<table>
<thead>
<tr>
<th>Command</th>
<th>Category</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>isolate-user-vlan enable</td>
<td>VLAN</td>
<td>2-3</td>
</tr>
<tr>
<td>isolate-user-vlan igsp enable</td>
<td>VLAN</td>
<td>2-4</td>
</tr>
<tr>
<td>key</td>
<td>Security</td>
<td>2-25</td>
</tr>
<tr>
<td>language-mode</td>
<td>Getting Started</td>
<td>1-11</td>
</tr>
<tr>
<td>lcd</td>
<td>System Management</td>
<td>1-24</td>
</tr>
<tr>
<td>line-rate</td>
<td>QoS/ACL</td>
<td>2-11</td>
</tr>
<tr>
<td>link-aggregation</td>
<td>Port</td>
<td>2-2</td>
</tr>
<tr>
<td>local-server</td>
<td>Security</td>
<td>2-26</td>
</tr>
<tr>
<td>local-user</td>
<td>Security</td>
<td>2-10</td>
</tr>
<tr>
<td>local-user</td>
<td>System Management</td>
<td>1-16</td>
</tr>
<tr>
<td>local-user password-display-mode</td>
<td>Security</td>
<td>2-11</td>
</tr>
<tr>
<td>lock</td>
<td>Getting Started</td>
<td>1-11</td>
</tr>
<tr>
<td>logging-host</td>
<td>Integrated Management</td>
<td>2-27</td>
</tr>
<tr>
<td>loopback</td>
<td>Port</td>
<td>1-11</td>
</tr>
<tr>
<td>loopback-detection control enable</td>
<td>Port</td>
<td>1-11</td>
</tr>
<tr>
<td>loopback-detection enable</td>
<td>Port</td>
<td>1-12</td>
</tr>
<tr>
<td>loopback-detection interval-time</td>
<td>Port</td>
<td>1-13</td>
</tr>
<tr>
<td>loopback-detection per-vlan enable</td>
<td>Port</td>
<td>1-13</td>
</tr>
<tr>
<td>ls</td>
<td>System Management</td>
<td>1-24</td>
</tr>
<tr>
<td>mac-address</td>
<td>System Management</td>
<td>2-2</td>
</tr>
<tr>
<td>mac-address max-mac-count</td>
<td>System Management</td>
<td>2-3</td>
</tr>
<tr>
<td>mac-address multicast</td>
<td>Multicast</td>
<td>4-1</td>
</tr>
<tr>
<td>mac-address timer</td>
<td>System Management</td>
<td>2-4</td>
</tr>
<tr>
<td>mdi</td>
<td>Port</td>
<td>1-14</td>
</tr>
<tr>
<td>messenger</td>
<td>Security</td>
<td>2-11</td>
</tr>
<tr>
<td>mirrored-to</td>
<td>QoS/ACL</td>
<td>2-12</td>
</tr>
<tr>
<td>Command</td>
<td>Category</td>
<td>Page</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------</td>
<td>------</td>
</tr>
<tr>
<td>mkdir</td>
<td>System Management</td>
<td>1-5</td>
</tr>
<tr>
<td>mkdir</td>
<td>System Management</td>
<td>1-25</td>
</tr>
<tr>
<td>move</td>
<td>System Management</td>
<td>1-6</td>
</tr>
<tr>
<td>move</td>
<td>System Management</td>
<td>1-6</td>
</tr>
<tr>
<td>multicast-source-deny</td>
<td>Multicast</td>
<td>2-10</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td></td>
<td></td>
</tr>
<tr>
<td>name</td>
<td>Security</td>
<td>2-12</td>
</tr>
<tr>
<td>nas-ip</td>
<td>Security</td>
<td>2-27</td>
</tr>
<tr>
<td>ndp enable</td>
<td>Integrated</td>
<td>2-4</td>
</tr>
<tr>
<td></td>
<td>Management</td>
<td></td>
</tr>
<tr>
<td>ndp timer aging</td>
<td>Integrated</td>
<td>2-5</td>
</tr>
<tr>
<td></td>
<td>Management</td>
<td></td>
</tr>
<tr>
<td>ndp timer hello</td>
<td>Integrated</td>
<td>2-5</td>
</tr>
<tr>
<td></td>
<td>Management</td>
<td></td>
</tr>
<tr>
<td>ndtp enable</td>
<td>Integrated</td>
<td>2-9</td>
</tr>
<tr>
<td></td>
<td>Management</td>
<td></td>
</tr>
<tr>
<td>ndtp explore</td>
<td>Integrated</td>
<td>2-10</td>
</tr>
<tr>
<td></td>
<td>Management</td>
<td></td>
</tr>
<tr>
<td>ndtp hop</td>
<td>Integrated</td>
<td>2-11</td>
</tr>
<tr>
<td></td>
<td>Management</td>
<td></td>
</tr>
<tr>
<td>ndtp timer</td>
<td>Integrated</td>
<td>2-12</td>
</tr>
<tr>
<td></td>
<td>Management</td>
<td></td>
</tr>
<tr>
<td>ndtp timer hop-delay</td>
<td>Integrated</td>
<td>2-12</td>
</tr>
<tr>
<td></td>
<td>Management</td>
<td></td>
</tr>
<tr>
<td>ndtp timer port-delay</td>
<td>Integrated</td>
<td>2-13</td>
</tr>
<tr>
<td></td>
<td>Management</td>
<td></td>
</tr>
<tr>
<td>ntp-service access</td>
<td>System Management</td>
<td>7-4</td>
</tr>
<tr>
<td>ntp-service authentication enable</td>
<td>System Management</td>
<td>7-5</td>
</tr>
<tr>
<td>ntp-service authentication-keyid</td>
<td>System Management</td>
<td>7-6</td>
</tr>
<tr>
<td>ntp-service broadcast-client</td>
<td>System Management</td>
<td>7-6</td>
</tr>
<tr>
<td>ntp-service broadcast-server</td>
<td>System Management</td>
<td>7-7</td>
</tr>
<tr>
<td>ntp-service in-interface disable</td>
<td>System Management</td>
<td>7-12</td>
</tr>
<tr>
<td>ntp-service max-dynamic-sessions</td>
<td>System Management</td>
<td>7-8</td>
</tr>
<tr>
<td>ntp-service multicast-client</td>
<td>System Management</td>
<td>7-8</td>
</tr>
<tr>
<td>ntp-service multicast-server</td>
<td>System Management</td>
<td>7-9</td>
</tr>
<tr>
<td>ntp-service refclock-master</td>
<td>System Management</td>
<td>7-10</td>
</tr>
<tr>
<td>ntp-service reliable authentication-keyid</td>
<td>System Management</td>
<td>7-11</td>
</tr>
</tbody>
</table>
ntp-service source-interface  System Management  7-12
ntp-service unicast-peer  System Management  7-13
ntp-service unicast-server  System Management  7-14

O

open  System Management  1-25

P

packet-filter  QoS/ACL  1-5
parity  Getting Started  1-12
passive  System Management  1-26
password  Security  2-13
password  System Management  1-16
peer-public-key end  System Management  8-5
ping  System Management  4-15
poe disable  Remote Power-feeding  1-3
poe legacy disable  Remote Power-feeding  1-4
poe max-power  Remote Power-feeding  1-5
poe mode  Remote Power-feeding  1-5
poe power-management  Remote Power-feeding  1-6
poe priority  Remote Power-feeding  1-7
poe update  Remote Power-feeding  1-7
port  VLAN  1-2
port access vlan  Port  1-15
port hybrid pvid vlan  Port  1-15
port hybrid vlan  Port  1-16
port link-type  Port  1-17
port trunk permit vlan  Port  1-17
port trunk pvid vlan  Port  1-18
<table>
<thead>
<tr>
<th>Command</th>
<th>Category</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>port-tagged</td>
<td>Integrated</td>
<td>2-28</td>
</tr>
<tr>
<td>primary accounting</td>
<td>Security</td>
<td>2-28</td>
</tr>
<tr>
<td>primary authentication</td>
<td>Security</td>
<td>2-29</td>
</tr>
<tr>
<td>priority</td>
<td>QoS/ACL</td>
<td>2-13</td>
</tr>
<tr>
<td>priority trust</td>
<td>QoS/ACL</td>
<td>2-14</td>
</tr>
<tr>
<td>protocol inbound</td>
<td>Getting Started</td>
<td>1-13</td>
</tr>
<tr>
<td>protocol inbound</td>
<td>System Management</td>
<td>8-6</td>
</tr>
<tr>
<td>public-key-code begin</td>
<td>System Management</td>
<td>8-7</td>
</tr>
<tr>
<td>public-key-code end</td>
<td>System Management</td>
<td>8-8</td>
</tr>
<tr>
<td>put</td>
<td>System Management</td>
<td>1-27</td>
</tr>
<tr>
<td>pwd</td>
<td>System Management</td>
<td>1-8</td>
</tr>
<tr>
<td>pwd</td>
<td>System Management</td>
<td>1-27</td>
</tr>
<tr>
<td>qos cos-local-precedence-map</td>
<td>QoS/ACL</td>
<td>2-14</td>
</tr>
<tr>
<td>queue-scheduler</td>
<td>QoS/ACL</td>
<td>2-16</td>
</tr>
<tr>
<td>quit</td>
<td>Getting Started</td>
<td>1-13</td>
</tr>
<tr>
<td>quit</td>
<td>System Management</td>
<td>1-28</td>
</tr>
<tr>
<td>radius nas-ip</td>
<td>Security</td>
<td>2-30</td>
</tr>
<tr>
<td>radius scheme</td>
<td>Security</td>
<td>2-31</td>
</tr>
<tr>
<td>radius-scheme</td>
<td>Security</td>
<td>2-14</td>
</tr>
<tr>
<td>reboot</td>
<td>System Management</td>
<td>3-6</td>
</tr>
<tr>
<td>reboot member</td>
<td>Integrated</td>
<td>2-29</td>
</tr>
<tr>
<td>region-name</td>
<td>STP</td>
<td>1-6</td>
</tr>
<tr>
<td>remotehelp</td>
<td>System Management</td>
<td>1-28</td>
</tr>
<tr>
<td>rename</td>
<td>System Management</td>
<td>1-8</td>
</tr>
<tr>
<td>reset acl counter</td>
<td>QoS/ACL</td>
<td>1-6</td>
</tr>
<tr>
<td>reset arp</td>
<td>Network Protocol</td>
<td>1-5</td>
</tr>
<tr>
<td>reset counters interface</td>
<td>Port</td>
<td>1-19</td>
</tr>
<tr>
<td>reset dot1x statistics</td>
<td>Security</td>
<td>1-17</td>
</tr>
<tr>
<td>reset garp statistics</td>
<td>VLAN</td>
<td>3-4</td>
</tr>
<tr>
<td>Command</td>
<td>Category</td>
<td>Page</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------</td>
<td>------</td>
</tr>
<tr>
<td>reset igmp-snooping statistics</td>
<td>Multicast</td>
<td>2-11</td>
</tr>
<tr>
<td>reset ip statistics</td>
<td>Network Protocol</td>
<td>6-8</td>
</tr>
<tr>
<td>reset logbuffer</td>
<td>System Management</td>
<td>4-31</td>
</tr>
<tr>
<td>reset ndp statistics</td>
<td>Integrated</td>
<td>2-6</td>
</tr>
<tr>
<td>reset poe-configuration</td>
<td>Remote Power-feeding</td>
<td>1-8</td>
</tr>
<tr>
<td>reset radius statistics</td>
<td>Security</td>
<td>2-32</td>
</tr>
<tr>
<td>reset recycle-bin</td>
<td>System Management</td>
<td>1-9</td>
</tr>
<tr>
<td>reset saved-configuration</td>
<td>System Management</td>
<td>1-12</td>
</tr>
<tr>
<td>reset stop-accounting-buffer</td>
<td>Security</td>
<td>2-32</td>
</tr>
<tr>
<td>reset stp</td>
<td>STP</td>
<td>1-7</td>
</tr>
<tr>
<td>reset tcp statistics</td>
<td>Network Protocol</td>
<td>6-9</td>
</tr>
<tr>
<td>reset traffic-statistic</td>
<td>QoS/ACL</td>
<td>2-17</td>
</tr>
<tr>
<td>reset trapbuffer</td>
<td>System Management</td>
<td>4-31</td>
</tr>
<tr>
<td>retry</td>
<td>Security</td>
<td>2-33</td>
</tr>
<tr>
<td>retry realtime-accounting</td>
<td>Security</td>
<td>2-34</td>
</tr>
<tr>
<td>retry stop-accounting</td>
<td>Security</td>
<td>2-35</td>
</tr>
<tr>
<td>return</td>
<td>Getting Started</td>
<td>1-14</td>
</tr>
<tr>
<td>revision-level</td>
<td>STP</td>
<td>1-8</td>
</tr>
<tr>
<td>rmdir</td>
<td>System Management</td>
<td>1-10</td>
</tr>
<tr>
<td>rmdir</td>
<td>System Management</td>
<td>1-29</td>
</tr>
<tr>
<td>rmon alarm</td>
<td>System Management</td>
<td>6-8</td>
</tr>
<tr>
<td>rmon event</td>
<td>System Management</td>
<td>6-9</td>
</tr>
<tr>
<td>rmon history</td>
<td>System Management</td>
<td>6-10</td>
</tr>
<tr>
<td>rmon prialarm</td>
<td>System Management</td>
<td>6-11</td>
</tr>
<tr>
<td>rmon statistics</td>
<td>System Management</td>
<td>6-12</td>
</tr>
<tr>
<td>rsa local-key-pair create</td>
<td>System Management</td>
<td>8-8</td>
</tr>
<tr>
<td>rsa local-key-pair destroy</td>
<td>System Management</td>
<td>8-9</td>
</tr>
<tr>
<td>rsa peer-public-key</td>
<td>System Management</td>
<td>8-10</td>
</tr>
<tr>
<td>rule</td>
<td>QoS/ACL</td>
<td>1-7</td>
</tr>
<tr>
<td>save</td>
<td>System Management</td>
<td>1-12</td>
</tr>
<tr>
<td>screen-length</td>
<td>Getting Started</td>
<td>1-14</td>
</tr>
<tr>
<td>Command</td>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------</td>
<td>------</td>
</tr>
<tr>
<td>secondary accounting</td>
<td>Security</td>
<td>2-36</td>
</tr>
<tr>
<td>secondary authentication</td>
<td>Security</td>
<td>2-36</td>
</tr>
<tr>
<td>self-service-url</td>
<td>Security</td>
<td>2-14</td>
</tr>
<tr>
<td>send</td>
<td>Getting Started</td>
<td>1-15</td>
</tr>
<tr>
<td>server-type</td>
<td>Security</td>
<td>2-37</td>
</tr>
<tr>
<td>service-type</td>
<td>Getting Started</td>
<td>1-15</td>
</tr>
<tr>
<td>service-type</td>
<td>Security</td>
<td>2-15</td>
</tr>
<tr>
<td>service-type</td>
<td>System Management</td>
<td>1-17</td>
</tr>
<tr>
<td>service-type multicast</td>
<td>Multicast</td>
<td>5-1</td>
</tr>
<tr>
<td>set authentication password</td>
<td>Getting Started</td>
<td>1-17</td>
</tr>
<tr>
<td>shell</td>
<td>Getting Started</td>
<td>1-18</td>
</tr>
<tr>
<td>shutdown</td>
<td>Getting Started</td>
<td>2-21</td>
</tr>
<tr>
<td>shutdown</td>
<td>Port</td>
<td>1-20</td>
</tr>
<tr>
<td>snmp-agent community</td>
<td>QoS/ACL</td>
<td>3-2</td>
</tr>
<tr>
<td>snmp-agent community</td>
<td>System Management</td>
<td>5-8</td>
</tr>
<tr>
<td>snmp-agent group</td>
<td>QoS/ACL</td>
<td>3-3</td>
</tr>
<tr>
<td>snmp-agent group</td>
<td>System Management</td>
<td>5-9</td>
</tr>
<tr>
<td>snmp-agent local-engineid</td>
<td>System Management</td>
<td>5-8</td>
</tr>
<tr>
<td>snmp-agent mib-view</td>
<td>System Management</td>
<td>5-10</td>
</tr>
<tr>
<td>snmp-agent packet max-size</td>
<td>System Management</td>
<td>5-11</td>
</tr>
<tr>
<td>snmp-agent sys-info</td>
<td>System Management</td>
<td>5-11</td>
</tr>
<tr>
<td>snmp-agent target-host</td>
<td>System Management</td>
<td>5-12</td>
</tr>
<tr>
<td>snmp-agent trap enable</td>
<td>System Management</td>
<td>5-13</td>
</tr>
<tr>
<td>snmp-agent trap life</td>
<td>System Management</td>
<td>5-14</td>
</tr>
<tr>
<td>snmp-agent trap queue-size</td>
<td>System Management</td>
<td>5-15</td>
</tr>
<tr>
<td>snmp-agent trap source</td>
<td>System Management</td>
<td>5-16</td>
</tr>
<tr>
<td>snmp-agent usm-user</td>
<td>QoS/ACL</td>
<td>3-4</td>
</tr>
<tr>
<td>snmp-agent usm-user</td>
<td>System Management</td>
<td>5-16</td>
</tr>
<tr>
<td>snmp-host</td>
<td>Integrated Management</td>
<td>2-29</td>
</tr>
<tr>
<td>speed</td>
<td>Getting Started</td>
<td>1-19</td>
</tr>
<tr>
<td>speed</td>
<td>Port</td>
<td>1-20</td>
</tr>
<tr>
<td>ssh server authentication-retries</td>
<td>System Management</td>
<td>8-11</td>
</tr>
<tr>
<td>ssh server rekey-interval</td>
<td>System Management</td>
<td>8-11</td>
</tr>
<tr>
<td>Command</td>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------</td>
<td>------</td>
</tr>
<tr>
<td>ssh server timeout</td>
<td>System Management</td>
<td>8-12</td>
</tr>
<tr>
<td>ssh user assign rsa-key</td>
<td>System Management</td>
<td>8-12</td>
</tr>
<tr>
<td>ssh user username authentication-type</td>
<td>System Management</td>
<td>8-13</td>
</tr>
<tr>
<td>stacking</td>
<td>Integrated Management</td>
<td>1-2</td>
</tr>
<tr>
<td>stacking enable</td>
<td>Integrated Management</td>
<td>1-3</td>
</tr>
<tr>
<td>stacking ip-pool</td>
<td>Integrated Management</td>
<td>1-3</td>
</tr>
<tr>
<td>state</td>
<td>Security</td>
<td>2-16</td>
</tr>
<tr>
<td>state</td>
<td>Security</td>
<td>2-38</td>
</tr>
<tr>
<td>stop-accounting-buffer enable</td>
<td>Security</td>
<td>2-39</td>
</tr>
<tr>
<td>stopbits</td>
<td>Getting Started</td>
<td>1-19</td>
</tr>
<tr>
<td>stp</td>
<td>STP</td>
<td>1-9</td>
</tr>
<tr>
<td>stp bpdu-protection</td>
<td>STP</td>
<td>1-9</td>
</tr>
<tr>
<td>stp bridge-diameter</td>
<td>STP</td>
<td>1-10</td>
</tr>
<tr>
<td>stp bridge-priority</td>
<td>STP</td>
<td>1-11</td>
</tr>
<tr>
<td>stp cost</td>
<td>STP</td>
<td>1-13</td>
</tr>
<tr>
<td>stp edged-port</td>
<td>STP</td>
<td>1-12</td>
</tr>
<tr>
<td>stp interface</td>
<td>STP</td>
<td>1-17</td>
</tr>
<tr>
<td>stp interface cost</td>
<td>STP</td>
<td>1-19</td>
</tr>
<tr>
<td>stp interface edged-port</td>
<td>STP</td>
<td>1-18</td>
</tr>
<tr>
<td>stp interface loop-protection</td>
<td>STP</td>
<td>1-22</td>
</tr>
<tr>
<td>stp interface mcheck</td>
<td>STP</td>
<td>1-22</td>
</tr>
<tr>
<td>stp interface point-to-point</td>
<td>STP</td>
<td>1-23</td>
</tr>
<tr>
<td>stp interface port priority</td>
<td>STP</td>
<td>1-21</td>
</tr>
<tr>
<td>stp interface root-protection</td>
<td>STP</td>
<td>1-24</td>
</tr>
<tr>
<td>stp interface transit-limit</td>
<td>STP</td>
<td>1-25</td>
</tr>
<tr>
<td>stp loop-protection</td>
<td>STP</td>
<td>1-26</td>
</tr>
<tr>
<td>stp max-hops</td>
<td>STP</td>
<td>1-27</td>
</tr>
<tr>
<td>stp mcheck</td>
<td>STP</td>
<td>1-27</td>
</tr>
<tr>
<td>stp mode</td>
<td>STP</td>
<td>1-28</td>
</tr>
<tr>
<td>stp point-to-point</td>
<td>STP</td>
<td>1-29</td>
</tr>
<tr>
<td>stp port priority</td>
<td>STP</td>
<td>1-14</td>
</tr>
<tr>
<td>stp region-configuration</td>
<td>STP</td>
<td>1-30</td>
</tr>
</tbody>
</table>
stp root primary STP 1-15
stp root secondary STP 1-16
stp root-protection STP 1-31
stp tc-protection STP 1-30
stp timer forward-delay STP 1-32
stp timer hello STP 1-33
stp timer max-age STP 1-34
stp transit-limit STP 1-35
super Getting Started 1-20
super password Getting Started 1-20
sysname Getting Started 1-21
sysname System Management 4-3
system-view Getting Started 1-22

tcp timer fin-timeout Network Protocol 6-9
tcp timer syn-timeout Network Protocol 6-10
tcp window Network Protocol 6-11
telnet Getting Started 1-22
temperature-limit System Management 3-7
terminal debugging System Management 4-31
terminal logging System Management 4-32
terminal monitor System Management 4-33
terminal trapping System Management 4-33
tftp System Management 1-30
tftp get System Management 1-31
tftp put System Management 1-31
tftp-server Integrated Management 2-30
timer Integrated Management 2-31
timer Security 2-40
timer quiet Security 2-41
timer realtime-accounting Security 2-41
time-range QoS/ACL 1-11
<table>
<thead>
<tr>
<th>Command</th>
<th>Category</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>tracert</td>
<td>System Management</td>
<td>4-17</td>
</tr>
<tr>
<td>traffic-limit</td>
<td>QoS/ACL</td>
<td>2-18</td>
</tr>
<tr>
<td>traffic-priority</td>
<td>QoS/ACL</td>
<td>2-20</td>
</tr>
<tr>
<td>traffic-redirect</td>
<td>QoS/ACL</td>
<td>2-21</td>
</tr>
<tr>
<td>traffic-statistic</td>
<td>QoS/ACL</td>
<td>2-22</td>
</tr>
<tr>
<td>undelete</td>
<td>System Management</td>
<td>1-10</td>
</tr>
<tr>
<td>undo snmp-agent</td>
<td>System Management</td>
<td>5-17</td>
</tr>
<tr>
<td>unknown-multicast drop enable</td>
<td>Multicast</td>
<td>3-1</td>
</tr>
<tr>
<td>user</td>
<td>System Management</td>
<td>1-29</td>
</tr>
<tr>
<td>user privilege level</td>
<td>Getting Started</td>
<td>1-24</td>
</tr>
<tr>
<td>user-interface</td>
<td>Getting Started</td>
<td>1-23</td>
</tr>
<tr>
<td>user-name-format</td>
<td>Security</td>
<td>2-42</td>
</tr>
<tr>
<td>verbose</td>
<td>System Management</td>
<td>1-29</td>
</tr>
<tr>
<td>vlan</td>
<td>VLAN</td>
<td>1-3</td>
</tr>
<tr>
<td>vlan { enable</td>
<td>disable }</td>
<td>VLAN</td>
</tr>
<tr>
<td>vlan-assignment-mode</td>
<td>Security</td>
<td>2-17</td>
</tr>
<tr>
<td>vlan-mapping modulo</td>
<td>STP</td>
<td>1-36</td>
</tr>
<tr>
<td>voice vlan</td>
<td>VLAN</td>
<td>4-3</td>
</tr>
<tr>
<td>voice vlan aging</td>
<td>VLAN</td>
<td>4-2</td>
</tr>
<tr>
<td>voice vlan enable</td>
<td>VLAN</td>
<td>4-3</td>
</tr>
<tr>
<td>voice vlan mac-address</td>
<td>VLAN</td>
<td>4-4</td>
</tr>
<tr>
<td>voice vlan mode</td>
<td>VLAN</td>
<td>4-5</td>
</tr>
<tr>
<td>voice vlan security enable</td>
<td>VLAN</td>
<td>4-6</td>
</tr>
</tbody>
</table>

Huawei Technologies Proprietary
A-18