HUAWEI

Quidway S3000-EI Series Ethernet Switches Operation Manual

VRP3.10

Quidway S3000-EI Series Ethernet Switches
Operation Manual

Manual Version	T2-081691-20050625-C-1.04
Product Version	VRP3.10
BOM	31161091

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

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.

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

Organization

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

- **Getting Started**

  This module introduces how to access the Ethernet Switch.

- **Port**

  This module introduces Ethernet port and link aggregation configuration.

- **VLAN**

  This module introduces VLAN, isolate-user-vlan, GARP, and GVRP configuration.

- **Multicast**

  This module introduces GMRP and IGMP Snooping configuration.

- **QoS/ACL**

  This module introduces QoS/ACL configuration.

- **Integrated Management**

  This module introduces integrated configuration.

- **STP**

  This module introduces STP configuration.

- **Security**

  This module introduces security configuration.

- **Network Protocol**

  This module introduces network protocol configuration, including ARP, DHCP Snooping, and IP performance configuration.

- **System Management**

  This module introduces system management and maintenance of Ethernet Switch, including file system management, system maintenance and network management configuration.

- **Remote Power-feeding**

  This module introduces remote power-feeding configuration.

- **Appendix**

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

Convention	Description
Arial	Normal paragraphs are in Arial.
Boldface	Headings are in **Boldface**.
`Courier New`	Terminal Display is in `Courier New`.

II. Command conventions

Convention	Description
Boldface	The keywords of a command line are in **Boldface**.
italic	Command arguments are in *italic*.
[ ]	Items (keywords or arguments) in square brackets [ ] are optional.
{ x | y | ... }	Alternative items are grouped in braces and separated by vertical bars. One is selected.
[x | y | ...]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected.
{ x | y | ... } *	Alternative items are grouped in braces and separated by vertical bars. A minimum of one or a maximum of all can be selected.
[x | y | ...] *	Optional alternative items are grouped in square brackets and separated by vertical bars. Many or none can be selected.
#	A line starting with the # sign is comments.

III. GUI conventions

Convention	Description
< >	Button names are inside angle brackets. For example, click the <OK> button.
[ ]	Window names, menu items, data table and field names are inside square brackets. For example, pop up the [New User] window.
/	Multi-level menus are separated by forward slashes. For example, [File/Create/Folder].

IV. Keyboard operation

Format	Description
<Key>	Press the key with the key name inside angle brackets. For example, <Enter>, <Tab>, <Backspace>, or <A>.
<Key1+Key2>	Press the keys concurrently. For example, <Ctrl+Alt+A> means the three keys should be pressed concurrently.
<Key1, Key2>	Press the keys in turn. For example, <Alt, A> means the two keys should be pressed in turn.

V. Mouse operation

Action	Description
Select	Press and hold the primary mouse button (left mouse button by default).
Click	Select and release the primary mouse button without moving the pointer.
Double-Click	Press the primary mouse button twice continuously and quickly without moving the pointer.
Drag	Press and hold the primary mouse button and move the pointer to a certain position.

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.

HUAWEI

Quidway S3000-EI Series Ethernet Switches
Operation Manual

Getting Started

Table of Contents

Chapter 1 Product Overview

1.1 Product Overview

Quidway S3000-EI Series Ethernet Switches, the L2 Ethernet Switches independently developed by Huawei, provide wire-speed L2 switching function. The series include the following main types of switches:

- S3026G Ethernet Switch
- S3026C Ethernet Switch
- S3026T Ethernet Switch
- S3026E FM Ethernet Switch
- S3026E FS Ethernet Switch
- S3026C-PWR Ethernet Switch

S3026G Ethernet Switch provides 24 fixed 10/100Base-TX auto-sensing ports, one Console port, and two GBIC extended module interfaces.

S3026C Ethernet Switch provides 24 fixed 10/100Base-TX auto-sensing ports, one Console port, and two extension module slots.

S3026T Ethernet Switch provides 24 fixed 10/100Base-TX auto-sensing ports, one Console port, and two fixed 10/100/1000Base-T uplink ports.

The only difference between S3026E FM and S3026E FS Ethernet Switch is the fixed optical ports with different attributes they provide: S3026E FM Ethernet Switch provides 12 fixed 100Base-FX multi-mode optical ports, while S3026E FS Ethernet Switch provides 12 fixed 100Base-FX single-mode optical ports. Each of them also provides one console port, two 6-port 100M extended module slots, and two uplink extended module slots.

S3026C-PWR Ethernet switch provides 24 fixed 10/100Base-TX auto-sensing port, one Console port and two extension module slots. S3026C-PWR switch can provide -48V DC power to remote powered device connected it through twisted pair cable, and then realizes remote power supply to remote connected powered device.

Quidway S3000-EI Series Ethernet Switches support the following services:

- Internet broadband access
- Enterprise and campus networking
- Providing multicast service function and supporting audio and video multicast services.

Hereinafter Quidway S3000-EI Series Ethernet Switches are referred to as S3000-EI Series Ethernet Switches.

1.2 Function Features

Table 1-1 Function features

Features	Implementation
VLAN	Supports VLAN compliant with IEEE 802.1Q Standard Supports port-based VLAN Supports GARP VLAN Registration Protocol (GVRP)
STP protocol	Supports Spanning Tree Protocol (STP) / Rapid Spanning Tree Protocol (RSTP)/ Multiple Spanning Tree Protocol (MSTP), compliant with IEEE 802.1D/IEEE802.1w/IEEE 802.1s Standard
Flow control	Supports IEEE 802.3 flow control (full-duplex) Supports back-pressure based flow control (half-duplex)
Broadcast Suppression	Supports Broadcast Suppression
Multicast	Supports GARP Multicast Registration Protocol (GMRP) Supports Internet Group Management Protocol (IGMP) Snooping
Link aggregation	Supports link aggregation
Mirror	Support the mirror based on the traffic classification
PoE	Support Power over Ethernet (PoE) only on the S3026C-PWR switch in S3000-EI series
Quality of Service (QoS)	Supports traffic classification Supports bandwidth control Supports priority Supports queues of different priority on the port Queue scheduling: supports Strict Priority Queuing (SP), Weighted Round Robin (WRR), Delay bounded WRR
Security features	Supports Multi-level User management and password protect Supports 802.1X authentication Supports packet filtering

Features	Implementation
Management and Maintenance	Supports command line interface configuration Supports configuration via Console port Supports remote configuration via Telnet or SSH Supports configuration through dialing the Modem Supports SNMP management (Supports Quidview NMS and RMON MIB Group 1, 2, 3 and 9) Supports system log Supports level alarms Supports Huawei Group Management Protocol (HGMP) V2 Supports output of the debugging information Supports PING and Tracert Supports the remote maintenance via Telnet or Modem or SSH
Loading and update	Supports to load and upgrade software via XModem protocol Supports to load and upgrade software via File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP)

Chapter 2 Logging in Switch

2.1 Setting up Configuration Environment via the Console Port

Step 1: As shown in the figure below, to set up the local configuration environment, connect the serial port of a PC (or a terminal) to the Console port of the switch with the Console cable.

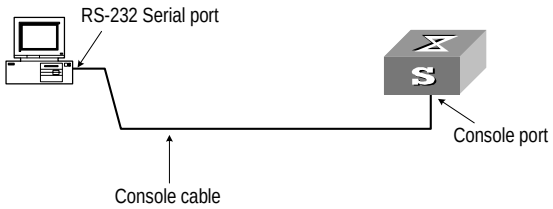


Figure 2-1 Setting up the local configuration environment via the Console port

Step 2: Run terminal emulator (such as Terminal on Windows 3X or the Hyper Terminal on Windows 9X) on the Computer. Set the terminal communication parameters as follows: Set the baud rate to 9600, databit to 8, parity check to none, stopbit to 1, flow control to none and select the terminal type as VT100.

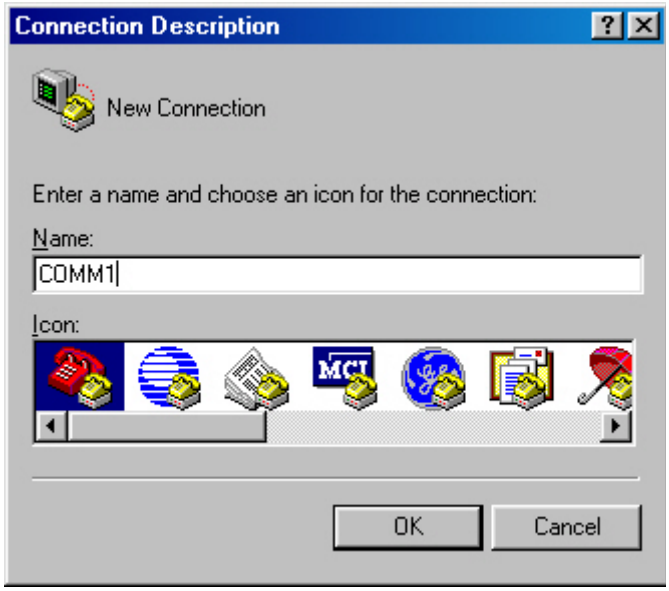


Figure 2-2 Setting up new connection

Figure 2-3 Configuring the port for connection

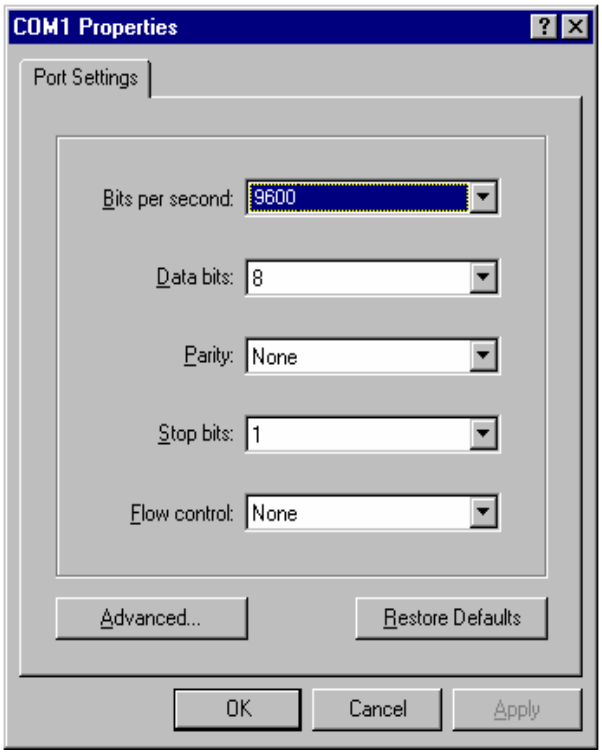


Figure 2-4 Setting communication parameters

Step 3: The switch is powered on. Display self-test information of the switch and prompt you to press Enter to show the command line prompt such as <Quidway>.

Step 4: Input a command to configure the switch or view the operation state. Input a “?” for an immediate help. For details of specific commands, refer to the following chapters.

2.2 Setting up Configuration Environment through Telnet

2.2.1 Connecting a PC to the Switch through Telnet

After you have correctly configured IP address of a VLAN interface for a switch via Console port (using **ip address** command in VLAN interface view), and added the port (that connects to a terminal) to this VLAN (using **port** command in VLAN view), you can telnet this switch and configure it.

Step 1: Authenticate the Telnet user via the Console port before the user logs in by Telnet.

Note:

By default, the password is required for authenticating the Telnet user to log in the switch. If a user logs in via the Telnet without password, he will see the prompt “Login password has not been set !”.

```
<Quidway> system-view
[Quidway] user-interface vty 0
[Quidway-ui-vty0] set authentication password simple xxxx (xxxx is the preset
login password of Telnet user)
```

Step 2: To set up the configuration environment, connect the Ethernet port of the PC to that of the switch via the LAN.

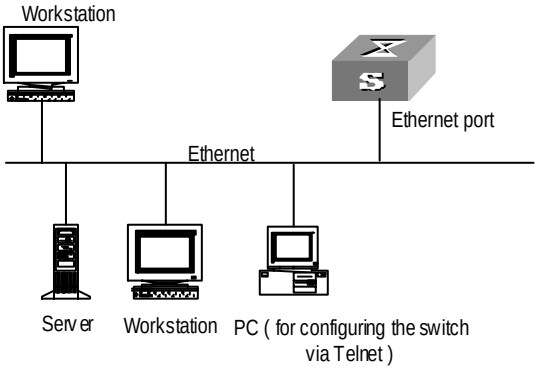


Figure 2-5 Setting up configuration environment through telnet

Step 3: Run Telnet on the PC and input the IP address of the VLAN connected to the PC port.

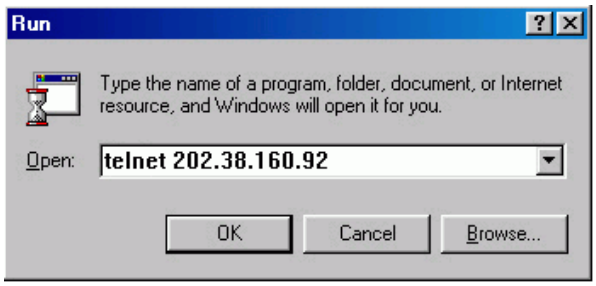


Figure 2-6 Running Telnet

Step 4: The terminal displays “Login authentication” and prompts the user to input the logon password. After you input the correct password, it displays the command line prompt (such as <Quidway>). If the prompt “All user interfaces are used, please try later!” appears, it indicates that too many users are connected to the switch through the Telnet at this moment. In this case, please reconnect later. At most 5 Telnet users are allowed to log on to the Quidway series switches simultaneously.

Step 5: Use the corresponding commands to configure the switch or to monitor the running state. Enter “?” to get the immediate help. For details of specific commands, refer to the following chapters.

Note:

- When configuring the switch via Telnet, do not modify the IP address of it unless necessary, for the modification might cut the Telnet connection.
- By default, when a Telnet user passes the password authentication to log on to the switch, he can access the commands at Level 0.

2.2.2 Telneting a Switch through another Switch

After a user has logged into a switch, he or she can configure another switch through the switch via Telnet. The local switch serves as Telnet client and the peer switch serves as Telnet server. If the ports connecting these two switches are in a same local network, their IP addresses must be configured in the same network segment. Otherwise, the two switches must establish a route that can reach each other.

As shown in the figure below, after you telnet to a switch, you can run telnet command to log in and configure another switch.

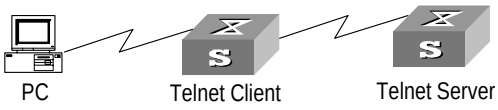


Figure 2-7 Providing Telnet Client service

Step 1: Authenticate the Telnet user via the Console port on the Telnet Server (switch) before login.

Note:

By default, the password is required for authenticating the Telnet user to log in the switch. If a user logs in via the Telnet without password, he will see the prompt “Login password has not been set !”.

```
<Quidway> system-view
[Quidway] user-interface vty 0
[Quidway-ui-vty0] set authentication password simple xxxx (xxxx is the preset
login password of Telnet user)
```

Step 2: The user logs in the Telnet Client (switch). For the login process, refer to the section describing “Connecting a PC to the Switch through Telnet”.

Step 3: Perform the following operations on the Telnet Client:

```
<Quidway> telnet xxxx (xxxx can be the hostname or IP address of the Telnet
Server. If it is the hostname, you need to use the ip host command to specify.)
```

Step 4: Enter the preset login password and you will see the prompt such <Quidway>. If the prompt “All user interfaces are used, please try later!” appears, it indicates that too many users are connected to the switch through the Telnet at this moment. In this case, please connect later.

Step 5: Use the corresponding commands to configure the switch or view it running state. Enter “?” to get the immediate help. For details of specific commands, refer to the following chapters.

2.3 Setting up Configuration Environment through a Dial-up the Modem

Step 1: Authenticate the Modem user via the Console port of the switch before he logs in the switch through a dial-up Modem.

Note:

By default, the password is required for authenticating the Modem user to log in the switch. If a user logs in via the Modem without password, he will see an error prompt.

```
<Quidway> system-view
[Quidway] user-interface aux 0
[Quidway-ui-aux0] set authentication password simple xxxx (xxxx is the preset
login password of the Modem user.)
```

Step 2: Perform the following configurations on the Modem that is directly connected to the switch. (You are not required to configure the Modem connected to the terminal.)

```
AT&F      ---------------------- Reset Modem factory settings
ATS0=1    -----------------Set auto response (ring once)
AT&D      ---------------------- Ignore DTR signal
AT&K0 -----------------        ------ Disable flow control
AT&R1     ---------------------- Ignore RTS signal
AT&S0 ----------------         ------- Force DSR to be high-level
ATEQ1&W   ---------------     -------- Bar the modem to send command response
or execution result and save the configurations
```

After the configuration, key in the **AT&V** command to verify the Modem settings.

Note:

- The Modem configuration commands and outputs may be different according to different Modems. For details, refer to the User Manual of the Modem.
- It is recommended that the transmission rate on the Console port must lower than that of Modem, otherwise packets may be lost.

Step 3: As shown in the figure below, to set up the remote configuration environment, connect the Modems to a PC (or a terminal) serial port and the switch Console port respectively.

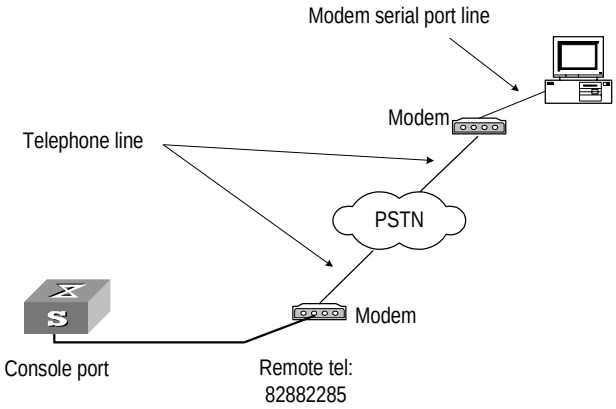


Figure 2-8 Setting up remote configuration environment

Step 4: Dial for connection to the switch, using the terminal emulator and Modem on the remote end. The number dialed shall be the telephone number of the Modem connected to the switch. See the two figures below.

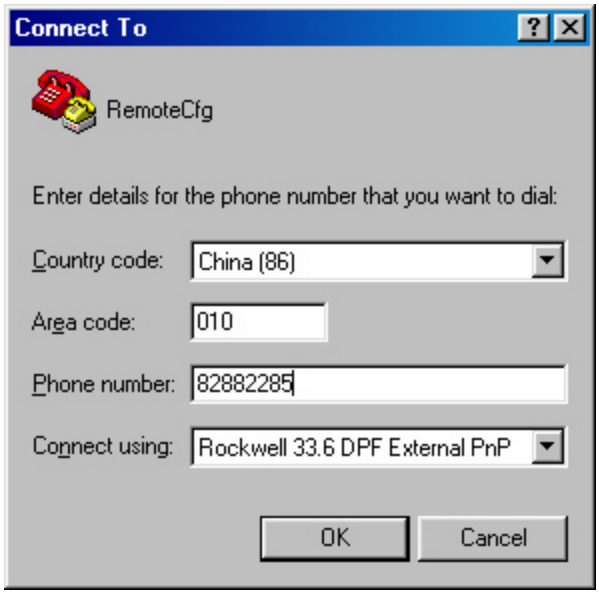


Figure 2-9 Setting the dialed number

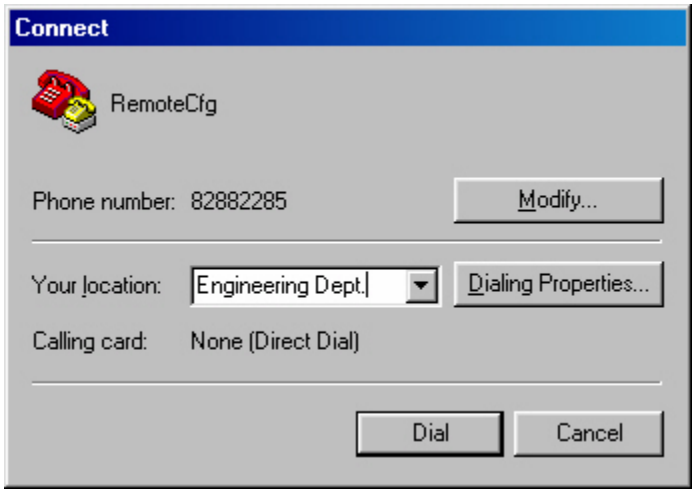


Figure 2-10 Dialing on the remote PC

Step 5: Enter the preset login password on the remote terminal emulator and wait for the prompt such as <Quidway>. Then you can configure and manage the switch. Enter "?" to get the immediate help. For details of specific commands, refer to the following chapters.

Note:

By default, when a Modem user logs in, he can access the commands at Level 0.

Chapter 3 Command Line Interface

3.1 Command Line Interface

Quidway series switches provide a series of configuration commands and command line interfaces for configuring and managing the switch. The command line interface has the following characteristics:

- Local configuration via the Console port.
- Local or remote configuration via Telnet or SSH.
- Remote configuration through a dial-up Modem to log in the switch.
- Hierarchy command protection to avoid the unauthorized users accessing switch.
- Enter a "?" to get immediate online help.
- Provide network testing commands, such as Tracert and Ping, to fast troubleshoot the network.
- Provide various detailed debugging information to help with network troubleshooting.
- Log in and manage other switch directly, using the Telnet command.
- Provide FTP service for the users to upload and download files.
- Provide the function similar to Doskey to execute a history command.
- The command line interpreter searches for target not fully matching the keywords. It is ok for you to key in the whole keyword or part of it, as long as it is unique and not ambiguous.

3.2 Command Line View

Quidway series switches provide hierarchy protection for the command lines to avoid unauthorized user accessing illegally.

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 to system maintenance, service fault diagnosis, etc. The operation of saving 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: They are commands that influence basis operation of the system and system support module, which plays a support 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.

At the same time, 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.

In order to prevent unauthorized users from illegal intrusion, user will be identified when switching from a lower level to a higher level with **super** [*level*] command. User ID authentication is performed when users at lower level switch to users at higher level. In other words, user password of the higher level is needed (Suppose the user has set the **super password** [**level** *level*] { **simple** | **cipher** } *password.*) 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.

Different command views are implemented according to different requirements. They are related to one another. For example, after logging in the switch, you will enter user view, in which you can only use some basic functions such as displaying the running state and statistics information. In user view, key in **system-view** to enter system view, in which you can key in different configuration commands and enter the corresponding views.

The command line provides the following views:

- User view
- System view
- Ethernet Port view
- VLAN view
- VLAN interface view
- LoopBack interface view
- Local-user view
- User interface view
- FTP Client view
- Cluster view
- MST region view
- RSA public key view
- RSA key code view
- Basic ACL view
- Advanced ACL view
- Layer-2 ACL view
- User-defined ACL view
- RADIUS server group view

- ISP domain view

The following table describes the function features of different views and the ways to enter or quit.

Table 3-1 Function feature of command view

Command view	Function	Prompt	Command to enter	Command to exit
User view	Show the basic information about operation and statistics	<Quidway>	Enter right after connecting the switch	**quit** disconnects to the switch
System view	Configure system parameters	[Quidway]	Key in **system-view** in user view	**quit or return** returns to user view
Ethernet Port view	Configure Ethernet port parameters	[Quidway-Ethernet0/1]	100M Ethernet port view Key in **interface ethernet** 0/1 in system view	**quit** returns to system view **return** returns to user view
		[Quidway-GigabitEthernet1/1]	GigabitEthernet port view Key in **interface gigabitethernet** 1/1 in system view	
VLAN view	Configure VLAN parameters	[Quidway-Vlan1]	Key in **vlan** 1 in system view	**quit** returns to system view **return** returns to user view
VLAN interface view	Configure IP interface parameters for a VLAN or a VLAN aggregation	[Quidway-Vlan-interface1]	Key in **interface vlan-interface** 1 in system view	**quit** returns to system view **return** returns to user view
Local-user view	Configure local user parameters	[Quidway-luser-user1]	Key in **local-user** user1 in system view	**quit** returns to system view **return** returns to user view
User interface view	Configure user interface parameters	[Quidway-ui0]	Key in **user-interface** 0 in system view	**quit** returns to system view **return** returns to user view
FTP Client view	Configure FTP Client parameters	[ftp]	Key in **ftp** in user view	**quit** returns to system view

Command view	Function	Prompt	Command to enter	Command to exit
Cluster view	Configure Cluster parameters	[Quidway-cluster]	Key in **cluster** in system view	**quit** returns to system view **return** returns to user view
MST region view	Configure MST region parameters	[Quidway-mst-region]	Key in **stp region-configuration** in system view	**quit** returns to system view **return** returns to user view
RSA public key view	Configure RSA public key of SSH user	[Quidway-rsa-public-key]	Key in **rsa peer-public-key** quidway003 in system view	**peer-public-key end** returns to system view
RSA key code view	Edit RSA public key of SSH user	[Quidway-rsa-key-code]	Key in **public-key-code begin** in RSA public key view	**public-key-code end** returns to RSA public key view
Basic ACL view	Define the rule of basic ACL	[Quidway-acl-basic-2000]	Key in **acl number** 2000 in system view	**quit** returns to system view **return** returns to user view
Advanced ACL view	Define the rule of advanced ACL	[Quidway-acl-adv-3000]	Key in **acl number** 3000 in system view	**quit** returns to system view **return** returns to user view
Layer-2 ACL view	Define the rule of layer-2 ACL	[Quidway-acl-link-4000]	Key in **acl number** 4000 in system view	**quit** returns to system view **return** returns to user view
User-defined ACL view	Define the rule of user-defined ACL	[Quidway-acl-user-5000]	Key in **acl number** 5000 in system view	**quit** returns to system view **return** returns to user view
Conform-level view	Configure the "DSCP + Conform-level Service group" mapping table and "Local-precedence + Conform-level 802.1p priority" mapping table	[Quidway-conform-level-0]	Key in **qos conform-level** 0 in system view	**quit** returns to system view **return** returns to user view
WRED index view	Configure WRED parameters	[Quidway-wred-0]	Key in **wred** 0 in system view	**quit** returns to system view **return** returns to user view

Command view	Function	Prompt	Command to enter	Command to exit
RADIUS server group view	Configure radius parameters	[Quidway-radius-1]	Key in **radius scheme** 1 in system view	**quit** returns to system view **return** returns to user view
ISP domain view	Configure ISP domain parameters	[Quidway-isp-huawei163.net]	Key in **domain** huawei163.net in system view	**quit** returns to system view **return** returns to user view

3.3 FeaturesFeature and Functions of Command Line

3.3.1 Online Help of Command Line

The command line interface provides the following online help modes.

- Full help
- Partial help

You can get the help information through these online help commands, which are described as follows.

1) Input "?" in any view to get all the commands in it and corresponding descriptions.

```
<Quidway> ?
User view commands:
  boot               Set boot option
  cd                 Change current directory
  clock              Specify the system clock
  copy               Copy from one file to another
  debugging          Enable system debugging functions
  delete             Delete a file
  dir                List files on a file system
  display            Display current system information
  (Omitted)
```

2) Input a command with a "?" separated by a space. If this position is for keywords, all the keywords and the corresponding brief descriptions will be listed.

```
<Quidway> language-mode ?
  chinese  Chinese environment
  english  English environment
```

3) Input a command with a "?" separated by a space. If this position is for parameters, all the parameters and their brief descriptions will be listed.

```
[Quidway] interface vlan ?
  <1-4094>  VLAN interface number
[Quidway] interface vlan 1 ?
```

```
  <cr>
<cr> indicates no parameter in this position. The next command line repeats
the command, you can press <Enter> to execute it directly.
```

4) Input a character string with a "?", then all the commands with this character string as their initials will be listed.

```
<Quidway>pi?
ping
```

5) Input a command with a character string and "?", then all the key words with this character string as their initials in the command will be listed.

```
<Quidway> display ver?
  version
```

6) Input the first letters of a keyword of a command and press <Tab> key. If no other keywords are headed by this letters, then this unique keyword will be displayed automatically.
7) To switch to the Chinese display for the above information, perform the **language-mode** command.

3.3.2 Displaying Characteristics of Command Line

Command line interface provides the following display characteristics:

- For users' convenience, the instruction and help information can be displayed in both English and Chinese.
- For the information to be displayed exceeding one screen, pausing function is provided. In this case, users can have three choices, as shown in the table below.

Table 3-2 Functions of displaying

Key or Command	Function
Press <Ctrl+C> when the display pauses	Stop displaying and executing command.
Enter a space when the display pauses	Continue to display the next screen of information.
Press <Enter> when the display pauses	Continue to display the next line of information.

3.3.3 History Command of Command Line

Command line interface provides the function similar to that of DosKey. The commands entered by users can be automatically saved by the command line interface and you can invoke and execute them at any time later. History command buffer is defaulted as 10. That is, the command line interface can store 10 history commands for each user. The operations are shown in the table below.

Table 3-3 Retrieving history command

Operation	Key	Result
Display history command	**display history-command**	Display history command by user inputting
Retrieve the previous history command	Up cursor key <↑> or <Ctrl+P>	Retrieve the previous history command, if there is any.
Retrieve the next history command	Down cursor key <↓> or <Ctrl+N>	Retrieve the next history command, if there is any.

Note:

Cursor keys can be used to retrieve the history commands in Windows 3.X Terminal and Telnet. However, in Windows 9X HyperTerminal, the cursor keys ↑ and ↓ do not work, because Windows 9X HyperTerminal defines the two keys differently. In this case, use the combination keys <**Ctrl+P**> and <**Ctrl+N**> instead for the same purpose.

3.3.4 Common Command Line Error Messages

All the input commands by users can be correctly executed, if they have passed the grammar check. Otherwise, error messages will be reported to users. The common error messages are listed in the following table.

Table 3-4 Common command line error messages

Error messages	Causes
Unrecognized command	Cannot find the command.
	Cannot find the keyword.
	Wrong parameter type.
	The value of the parameter exceeds the range.
Incomplete command	The input command is incomplete.
Too many parameters	Enter too many parameters.
Ambiguous command	The parameters entered are not specific.

3.3.5 Editing Characteristics of Command Line

Command line interface provides the basic command editing function and supports to edit multiple lines. A command cannot longer than 256 characters. See the table below.

Table 3-5 Editing functions

Key	Function
Common keys	Insert from the cursor position and the cursor moves to the right, if the edition buffer still has free space.
Backspace	Delete the character preceding the cursor and the cursor moves backward.
Leftwards cursor key <←> or <Ctrl+B>	Move the cursor a character backward
Rightwards cursor key <→> or <Ctrl+F>	Move the cursor a character forward
Up cursor key <↑> or <Ctrl+P> Down cursor key <↓> or <Ctrl+N>	Retrieve the history command.
<Tab>	Press <Tab> after typing the incomplete key word and the system will execute the partial help: If the key word matching the typed one is unique, the system will replace the typed one with the complete key word and display it in a new line; if there is not a matched key word or the matched key word is not unique, the system will do no modification but display the originally typed word in a new line.

Chapter 4 User Interface Configuration

4.1 User Interface Overview

User interface configuration is another way provided by the switch to configure and manage the port data.

S3000-EI Series Ethernet Switches support the following configuration methods:

- Local configuration via the Console port
- Local and remote configuration through Telnet or SSH on Ethernet port
- Remote configuration through dial with modem via the Console port.

According to the above-mentioned configuration methods, there are two types of user interfaces:

- AUX user interface

AUX user interface is used to log in the switch via the Console port. A switch can only have one AUX user interface.

- VTY user interface

VTY user interface is used to telnet the switch. A switch can have up to five VTY user interface.

Note:

For Quidway series switches, AUX port and Console port are the same one. There is only the type of AUX user interface.

User interface is numbered in the following two ways: absolute number and relative number.

1) Absolute number, following the rules below.
- AUX user interface is numbered as the first interface designated as user interface 0.
- VTY is numbered after AUX user interface. The absolute number of the first VTY is incremented by 1 than the AUX user interface number.

2) Relative number, represented by "+ number" assigned to each type of user interface. It follows the rules below:
- Number of AUX user interface: AUX 0.
- Number of VTY: The first VTY interface is designated as VTY 0, the second one is designated as VTY 1, and so on.

4.2 User Interface Configuration

User interface configuration includes:

- Entering user interface view
- Configuring the user interface-supported protocol
- Configuring the attributes of AUX (Console) port
- Configuring the terminal attributes
- Managing users
- redirection

4.2.1 Entering User Interface View

The following command is used for entering a user interface view. You can enter a single user interface view or multi user interface view to configure one or more user interfaces respectively.

Perform the following configuration in system view.

Table 4-1 Entering user interface view

Operation	Command
Enter a single user interface view or multi user interface views	**user-interface** [*type*] *first-number* [*last-number*]

4.2.2 Configuring the User Interface-Supported Protocol

The following command is used for setting the supported protocol by the current user interface. You can log in switch only through the supported protocol. The configuration becomes effective when you log in again.

Perform the following configurations in user interface (VTY user interface only) view.

Table 4-2 Configuring the user interface-supported protocol

Operation	Command
Configure the user interface-supported protocol	**protocol inbound** { **all** | **ssh** | **telnet** }

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

Caution:

- If Telnet protocol is specified, to ensure a successful login via the Telnet, you must configure the password by default.
- If SSH protocol is specified, to ensure a successful login, you must configure the local or remote authentication of username and password using the **authentication-mode scheme** command. The **protocol inbound ssh** configuration fails if you configure **authentication-mode password** and **authentication-mode none**. When you configure SSH protocol successfully for the user interface, then you cannot configure **authentication-mode password** and **authentication-mode none** any more.

4.2.3 Configuring the Attributes of AUX (Console) Port

The following commands can be used for configuring the attributes of the AUX (Console) port, including speed, flow control, parity, stop bit and data bit.

Perform the following configurations in user interface (AUX user interface only) view.

I. Configuring the transmission speed on AUX (Console) port

Table 4-3 Configuring the transmission speed on AUX (Console) port

Operation	Command
Configure the transmission speed on AUX (Console) port	**speed** *speed-value*
Restore the default transmission speed on AUX (Console) port	**undo speed**

By default, the transmission speed on AUX (Console) port is 9600bps.

II. Configuring the flow control on AUX (Console) port

Table 4-4 Configuring the flow control on AUX (Console) port

Operation	Command
Configure the flow control on AUX (Console) port	**flow-control** { **hardware** | **none** | **software** }
Restore the default flow control mode on AUX (Console) port	**undo flow-control**

By default, the flow control on the AUX (Console) port is none, that is, no flow control will be performed.

III. Configuring parity on the AUX (Console) port

Table 4-5 Configuring parity on the AUX (Console) port

Operation	Command
Configure parity mode on the AUX (Console) port	**parity** { **even** | **mark** | **none** | **odd** | **space** }
Restore the default parity mode	**undo parity**

By default, the parity on the AUX (Console) port is none, that is, no parity bit.

IV. Configuring the stop bit of AUX (Console) port

Table 4-6 Configuring the stop bit of AUX (Console) port

Operation	Command
Configure the stop bit of AUX (Console) port	**stopbits** { **1** | **1.5** | **2** }
Restore the default stop bit of AUX (Console) port	**undo stopbits**

By default, AUX (Console) port supports 1 stop bit.

V. Configuring the data bit of AUX (Console) port

Table 4-7 Configuring the data bit of AUX (Console) port

Operation	Command
Configure the data bit of AUX (Console) port	**databits** { **7** | **8** }
Restore the default data bit of AUX (Console) port	**undo databits**

By default, AUX (Console) port supports 8 data bits.

4.2.4 Configuring the Terminal Attributes

The following commands can be used for configuring the terminal attributes, including enabling/disabling terminal service, disconnection upon timeout, lockable user interface, configuring terminal screen length and history command buffer size.

Perform the following configuration in user interface view. Perform **lock** command in user view.

I. Enabling/disabling terminal service

After the terminal service is disabled on a user interface, you cannot log in to the switch through the user interface. However, the user logged in through the user interface before disabling the terminal service can continue his operation. After such user logs

out, he cannot log in again. In this case, a user can log in to the switch through the user interface only when the terminal service is enabled again.

Table 4-8 Enabling/disabling terminal service

Operation	Command
Enable terminal service	**shell**
Disable terminal service	**undo shell**

By default, terminal service is enabled on all the user interfaces.

Note the following points:

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

II. Configuring idle-timeout

Table 4-9 Configuring idle-timeout

Operation	Command
Configure idle-timeout	**idle-timeout** *minutes* [*seconds*]
Restore the default idle-timeout	**undo idle-timeout**

By default, idle-timeout is enabled and set to 10 minutes on all the user interfaces. That is, the user interface will be disconnected automatically after 10 minutes without any operation.

idle-timeout 0 means disabling idle-timeout.

III. Locking the user interface

This configuration is to lock the current user interface and prompt the user to enter the password. This makes it impossible for others to operate in the interface after the user leaves.

Table 4-10 Locking the user interface

Operation	Command
Lock user interface	**lock**

IV. Setting the screen length

If a command displays more than one screen of information, you can use the following command to set how many lines to be displayed in a screen, so that the information can be separated in different screens and you can view it more conveniently.

Table 4-11 Setting the screen length

Operation	Command
Set the screen length	**screen-length** *screen-length*
Restore the default screen length	**undo screen-length**

By default, the terminal screen length is 24 lines.

screen-length 0 indicates to disable screen display separation function.

V. Setting the history command buffer size

Table 4-12 Setting the history command buffer size

Operation	Command
Set the history command buffer size	**history-command max-size** *value*
Restore the default history command buffer size	**undo history-command max-size**

By default, the size of the history command buffer is 10, that is, 10 history commands can be saved.

4.2.5 Managing Users

The management of users includes the setting of user logon authentication method, level of command which a user can use after logging on, level of command which a user can use after logging on from the specifically user interface, and command level.

I. Configuring the authentication method

The following command is used for configuring the user login authentication method to deny the access of an unauthorized user.

Perform the following configuration in user interface view.

Table 4-13 Configuring the authentication method

Operation	Command
Configure the authentication method	**authentication-mode** { **password** | **scheme** }
Configure no authentication	**authentication-mode none**

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

1) Perform local password authentication to the user interface

Using **authentication-mode password** command, you can perform local password authentication. That is, you need use the command below to configure a login password in order to login successfully.

Perform the following configuration in user interface view.

Table 4-14 Configuring the local authentication password

Operation	Command
Configure the local authentication password	**set authentication password** { **cipher** | **simple** }*password*
Remove the local authentication password	**undo set authentication password**

Configure for password authentication when a user logs in through a VTY 0 user interface and set the password to huawei.

```
[Quidway] user-interface vty 0
[Quidway-ui-vty0] authentication-mode password
[Quidway-ui-vty0] set authentication password simple huawei
```

2) Perform local or remote authentication of username and password to the user interface

Using **authentication-mode scheme** command, you can perform local or remote authentication of username and password. The type of the authentication depends on your configuration. For detailed information, see “Security” section.

In the following example, local username and password authentication are configured.

Perform username and password authentication when a user logs in through VTY 0 user interface and set the username and password to zbr and huawei respectively.

```
[Quidway-ui-vty0] authentication-mode scheme
[Quidway-ui-vty0] quit
[Quidway] local-user zbr
[Quidway-luser-zbr] password simple huawei
[Quidway-luser-zbr] service-type telnet
```

3) No authentication

```
[Quidway-ui-vty0] authentication-mode none
```

Note:

By default, the password is required for authenticating the Modem and Telnet users when they log in. If the password has not been set, when a user logs in, he will see the prompt “Login password has not been set !”.

If the **authentication-mode none** command is used, the Modem and Telnet users will not be required to input password.

II. Setting the command level used after a user logging in

The following command is used for setting the command level used after a user logging in.

Perform the following configuration in local-user view.

Table 4-15 Setting the command level used after a user logging in

Operation	Command
Set command level used after a user logging in	**service-type** { **ftp** [**ftp-directory** *directory*] | **lan-access** | **ssh** [**level** *level* | **telnet** [**level** *level*]] | **telnet** [**level** *level* | **ssh** [**level** *level*]] }
Restore the default command level used after a user logging in	**undo service-type** { **ftp** [**ftp-directory**] | **lan-access** | **ssh** [**level** | **telnet** [**level**]] | **telnet** [**level** | **ssh** [**level**]] }

By default, the specified logon user can access the commands at Level 1.

III. Setting the command level used after a user logs in from a user interface

You can use the following command to set the command level after a user logs in from a specific user interface, so that a user is able to execute the commands at such command level.

Perform the following configuration in user interface view.

Table 4-16 Setting the command level used after a user logging in from a user interface

Operation	Command
Set command level used after a user logging in from a user interface	**user privilege level** *level*
Restore the default command level used after a user logging in from a user interface	**undo user privilege level**

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.

Note:

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.

IV. Set command priority

The following command is used for setting the priority of a specified command in a certain view. The command levels include visit, monitoring, system, and management, which are identified with 0 through 3 respectively. An administrator assigns authorities as per user requirements.

Perform the following configuration in system view.

Table 4-17 Setting the command priority

Operation	Command
Set the command priority in a specified view.	**command-privilege level** *level* **view** *view command*
Restore the default command level in a specified view.	**Undo command-privilege view** *view command*

Note:

Please do not change the command level at will for it may cause inconvenience of maintenance and operation.

4.2.6 Configure Redirection

I. send command

The following command can be used for sending messages between user interfaces.

Perform the following configuration in user view.

Table 4-18 Configuring to send messages between different user interfaces.

Operation	Command
Configuring to send messages between different user interfaces.	**send** { **all** | *number* | *type number* }

II. auto-execute command

The following command is used to automatically run a command after you log in. After a command is configured to be run automatically, it will be automatically executed when you log in again.

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

Perform the following configuration in user interface view.

Table 4-19 Configuring to automatically run the command

Operation	Command
Configure to automatically run the command	**auto-execute command** *text*
Configure not to automatically run the command	**undo auto-execute command**

Note the following points:

- After executing this command, the user interface can no longer be used to carry out the routine configurations for the local system. Use this command with caution.
- Make sure that you will be able to log in the system in some other way and cancel the configuration, before you use the **auto-execute command** command and save the configuration.

Telnet 10.110.100.1 after the user logs in through VTY0 automatically.

```
[Quidway-ui-vty0] auto-execute command telnet 10.110.100.1
```

When a user logs on via VTY 0, the system will run **telnet** 10.110.100.1 automatically.

4.3 Displaying and Debugging User Interface

After the above configuration, execute **display** command in any view to display the running of the user interface configuration, and to verify the effect of the configuration.

Execute **free** command in user view to clear a specified user interface.

Table 4-20 Displaying and debugging user interface

Operation	Command
Clear a specified user interface	**free user-interface** [*type*] *number*
Display the user application information of the user interface	**display users** [**all**]
Display the physical attributes and some configurations of the user interface	**display user-interface** [*type number*] [*number*]

Chapter 5 System IP Configuration

5.1 System IP Overview

5.1.1 Management VLAN

Before performing remote management such as Telnet and web management, the IP address of the switch has to be configured first. For the Quidway series Layer 2 Ethernet switch, only one VLAN interface can be configured with an IP address, and the VLAN that corresponds to this interface becomes the management VLAN.

5.1.2 IP Address

I. IP address classification and indications

IP address is a 32-bit address allocated to the devices which access into the Internet. It consists of two fields: net-id field and host-id field. There are five types of IP address. See the following figure.

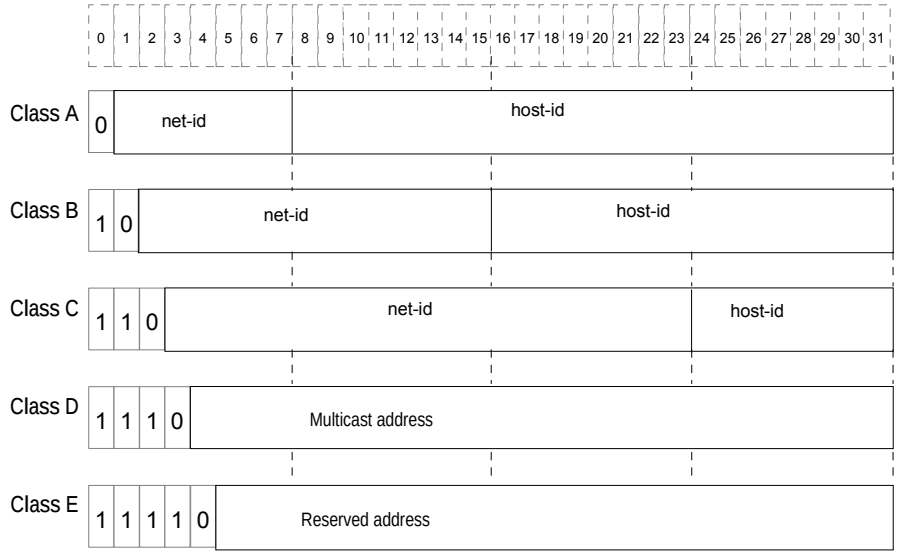


Figure 5-1 Five classes of IP address

Where, Class A, Class B and Class C are unicast addresses, while Class D addresses are multicast ones and class E addresses are reserved for special applications in future. The first three types are commonly used.

The IP address is in dotted decimal format. Each IP address contains 4 integers in dotted decimal notation. Each integer corresponds to one byte, e.g.10.110.50.101.

When using IP addresses, it should also be noted that some of them are reserved for special uses, and are seldom used. The IP addresses you can use are listed in the following table.

Table 5-1 IP address classes and ranges

Network class	Address range	IP network range	Note
A	0.0.0.0 to 127.255.255.255	1.0.0.0 to 126.0.0.0	Host ID with all the digits being 0 indicates that the IP address is the network address, and is used for network routing. Host ID with all the digits being 1 indicates the broadcast address, i.e. broadcast to all hosts on the network. IP address 0.0.0.0 is used for the host that is not put into use after starting up. The IP address with network number as 0 indicates the current network and its network can be cited by the router without knowing its network number. Network ID with the format of 127.X.Y.Z is reserved for self-loop test and the packets sent to this address will not be output to the line. The packets are processed internally and regarded as input packets.
B	128.0.0.0 to 191.255.255.255	128.0.0.0 to 191.254.0.0	Host ID with all the digits being 0 indicates that the IP address is the network address, and is used for network routing. Host ID with all the digits being 1 indicates the broadcast address, i.e. broadcast to all hosts on the network.
C	192.0.0.0 to 223.255.255.255	192.0.0.0 to 223.255.254.0	Host ID with all the digits being 0 indicates that the IP address is the network address, and is used for network routing. Host ID with all the digits being 1 indicates the broadcast address, i.e. broadcast to all hosts on the network.
D	224.0.0.0 to 239.255.255.255	None	Addresses of class D are multicast addresses.
E	240.0.0.0 to 255.255.255.254	None	The addresses are reserved for future use.

Network class	Address range	IP network range	Note
Other addresses	255.255.255.255	255.255.255.255	255.255.255.255 is used as LAN broadcast address.

II. Subnet and mask

Nowadays, with rapid development of the Internet, IP addresses are depleting very fast. The traditional IP address allocation method wastes IP addresses greatly. In order to make full use of the available IP addresses, the concept of mask and subnet is proposed.

A mask is a 32-bit number corresponding to an IP address. The number consists of 1s and 0s. Principally, these 1s and 0s can be combined randomly. However, the first consecutive bits are set to 1s when designing the mask. The mask divides the IP address into two parts: subnet address and host address. The bits 1s in the address and the mask indicate the subnet address and the other bits indicate the host address. If there is no sub-net division, then its sub-net mask is the default value and the length of "1" indicates the net-id length. Therefore, for IP addresses of classes A, B and C, the default values of corresponding sub-net mask are 255.0.0.0, 255.255.0.0 and 255.255.255.0 respectively.

The mask can be used to divide a Class A network containing more than 16,000,000 hosts or a Class B network containing more than 60,000 hosts into multiple small networks. Each small network is called a subnet. For example, for the Class B network address 138.38.0.0, the mask 255.255.224.0 can be used to divide the network into 8 subnets: 138.38.0.0, 138.38.32.0, 138.38.64.0, 138.38.96.0, 138.38.128.0, 138.38.160.0, 138.38.192.0 and 138.38.224.0 (Refer to the following figure). Each subnet can contain more than 8000 hosts.

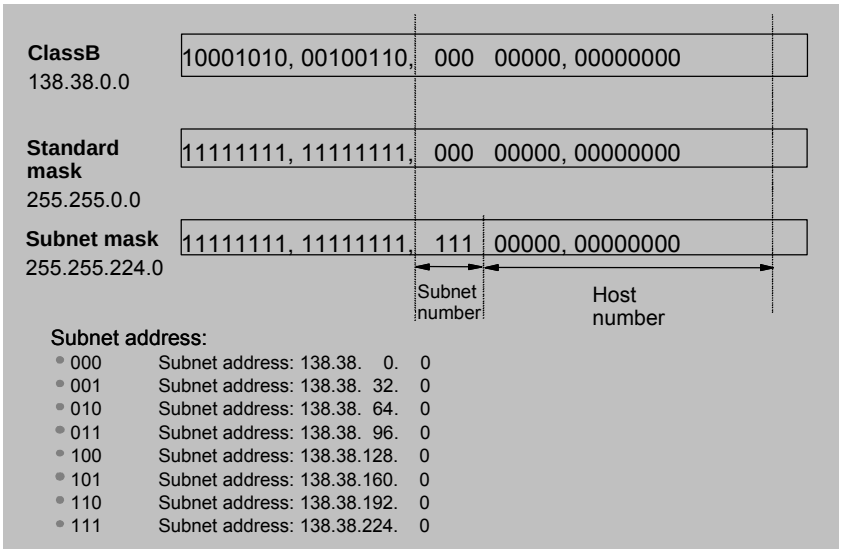


Figure 5-2 Subnet division of IP address

5.1.3 Static Route

A static route is a special route, which is manually configured by the network administrator. The static route is applied in a comparatively simple network. The proper configuration and usage of the static route can improve the network performance and ensure the bandwidth of the important applications.

Huawei Layer 2 Series Ethernet Switches can be configured with static route, used for login to the switch through the network.

5.2 System IP Configuration

System IP configuration includes:

- Creating/deleting a Management VLAN Interface
- Assigning/deleting the IP Address for/of the Management VLAN Interface
- Setting/deleting the management VLAN interface description character string
- Enabling/disabling a management VLAN interface
- Configuring the Hostname and Host IP Address
- Configuring a static route
- Configuring the default preference of static routes

5.2.1 Creating/Deleting a Management VLAN Interface

Perform the following configuration in system view.

Table 5-2 Creating/deleting a management VLAN interface

Operation	Command
Create a management VLAN interface and enter its view	**interface vlan-interface** *vlan-id*
Delete a management VLAN interface	**undo interface vlan-interface** *vlan-id*

Note that, user create a VLAN specified with the *vlan-id* parameter before perform this configuration task. But VLAN1 is the default VLAN, which you need not create.

5.2.2 Assigning/Deleting the IP Address for/of the Management VLAN Interface

You can use the following command to configure the IP address for the management VLAN interface, thus to perform remote management such as Telnet and web management to switch.

Perform the following configuration in VLAN interface view.

Table 5-3 Assigning/deleting the IP address for/of the management VLAN interface

Operation	Command
Assign the IP address of a management VLAN interface	**ip address** *ip-address net-mask*
Delete the IP address of a management VLAN interface	**undo ip address** [*ip-address net-mask*]

By default, the management VLAN interface has no IP address.

5.2.3 Setting/Deleting the Management VLAN Interface Description Character String

You can use the following command to set/delete management VLAN interface description character string.

Perform the following configuration in VLAN interface view.

Table 5-4 Setting/deleting the management VLAN interface description character string

Operation	Command
Set the description character string for management VLAN interface	**description string**
Restore the default description character string of management VLAN interface	**undo description string**

By default, the description character string is HUAWEI, Quidway Series, Vlan-interface1 Interface. Vlan-interface1 is the management VLAN interface name.

5.2.4 Enabling/Disabling a Management VLAN Interface

The following command can be used for disabling or enabling the management VLAN interface. After configuring the related parameters and protocol of the management VLAN interface, you can use the following command to enable the management VLAN interface. If you do not want the management VLAN interface to take effect, use the command to disable it.

Perform the following configuration in VLAN interface view.

Table 5-5 Enabling/disabling a management VLAN interface

Operation	Command
Disable management VLAN interface	**shutdown**
Enable management VLAN interface	**undo shutdown**

The operation of enabling/disabling management VLAN interface has no effect on the up/down status of the Ethernet ports belong to the VLAN.

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.

5.2.5 Configuring the Hostname and Host IP Address

You can use the following command to associate the hostname and host IP address. Thereafter you can simple use the hostname, instead of the meaningless IP address, when you perform the applications such as Telnet. And the system will translate the address for you.

Perform the following configuration in system view.

Table 5-6 Configuring the hostname and host IP address

Operation	Command
Configure a hostname and host IP address	**ip host** *hostname ip-address*
Delete a hostname and host IP address	**undo ip host** *hostname* [*ip-address*]

By default, there is no hostname associated with any host IP address.

5.2.6 Configuring a Static Route

You can use the following command to configure a static route for login to the switch via the network.

Perform the following configuration in system view.

Table 5-7 Configuring a static route

Operation	Command
Add a static route	**ip route-static** *ip-address* { *mask* | *mask-length* } { **null** *null-interface-number* | *gateway-address* } [**preference** *preference-value*]
Delete a static route	**undo ip route-static** *ip-address* { *mask* | *mask-length* } [**null** *null-interface-number* | *gateway-address*] [**preference** *preference-value*]

5.2.7 Configuring the Default Preference of Static Routes

The default-preference will be the preference of the static route if its preference is not specified when configured. You can change the default preference value of the static routes to be configured by using the following command.

Perform the following configurations in system view.

Table 5-8 Configuring the default preference of static routes

Operation	Command
Configure the default preference value of static routes	**ip route-static default-preference** *default-preference-value*
Remove the default preference value of static routes configure	**undo ip route-static default-preference**

By default, its value is 60.

5.3 Displaying and Debugging System IP

After the above configuration, execute **display** command in any view to display the running of the system IP configuration, and to verify the effect of the configuration.

Table 5-9 Displaying and debugging system IP

Operation	Command
View all the hosts and their IP addresses on the network	**display ip host**
View related IP information of the management VLAN interface	**display ip interface vlan-interface** *vlan-id*
View related information of the management VLAN interface	**display interface vlan-interface** [*vlan_id*]
View routing table summary	**display ip routing-table**
View routing table details	**display ip routing-table verbose**
View the detailed information of a specific route	**display ip routing-table** *ip-address* [*mask*] [**longer-match**] [**verbose**]
view the route information in the specified address range	**display ip routing-table** *ip_address1 mask1 ip_address2 mask2* [**verbose**]
View the route filtered through specified basic access control list (ACL)	**display ip routing-table acl** { *acl-number* | *acl-name* } [**verbose**]
View the route information that through specified ip prefix list	**display ip routing-table ip-prefix** *ip-prefix-name* [**verbose**]
View the routing information found by the specified protocol	**display ip routing-table protocol** *protocol* [**inactive** | **verbose**]
View the tree routing table	**display ip routing-table radix**
View the statistics of the routing table	**display ip routing-table statistics**

HUAWEI

Quidway S3000-EI Series Ethernet Switches
Operation Manual

Port

Table of Contents

Chapter 1 Ethernet Port Configuration

1.1 Ethernet Port Overview

S3026G Ethernet Switch provides 24 10/100Base-T fixed Ethernet ports and two GBIC uplink ports. You can select the gigabit optical module.

S3026C Ethernet Switch provides 24 10/100Base-T fixed Ethernet ports and two extended module slots and supports 100Base-FX Multi-mode module, 100Base-FX Single Mode module, 1000Base-SX module, 1000Base-LX module, 1000Base-T module, 1000Base-ZX module, 1000Base-LX GL module and stack module.

S3026T Ethernet Switch provides 24 10/100Base-T fixed Ethernet ports and two 10/100/1000Base-T uplink Ethernet ports.

The only difference between S3026E FM and S3026E FS Ethernet Switch is the fixed optical ports with the different attributes they provide: S3026E FM Ethernet Switch provides 12 fixed 100Base-FX multi-mode Ethernet ports. S3026E FS Ethernet Switch provides 12 fixed 100Base-FX single-mode Ethernet ports. Each of them also provides two 6-port 100M module slots and two uplink module slots. The 6-port 100M module slots support 6-port 10/100Base-T module, 6-port 100Base-FX single-mode module and 6-port 100Base-FX multi-mode module. The uplink module slots support 100Base-FX multi-mode module, 100Base-FX single-mode module, 1000Base-SX module, 1000Base-LX module, 1000Base-T electrical port module, 1000Base-ZX module, 1000Base-LX GL module, and stack module.

S3026C-PWR Ethernet switch provides 24 fixed 10/100Base-T fixed Ethernet ports and two extended module slots, which support one-port 1000Base-LX module, one-port 1000Base-SX module, one-port 1000Base-T module, one-port gigabit long haul/ medium haul optical interface module, one-port gigabit stack module, one-port 100Base-T single mode/multi-mode optical interface module, one-port 100Base-FX single mode medium haul optical interface module, one-port 100Base-T SFP interface module, and one-port gigabit GBIC interface module.

S3000-EI Series Ethernet Switches support the following Ethernet port features:

- 10/100Base-T Ethernet port supports MDI/MDI-X auto-sensing. It operates in half-duplex, full-duplex, or auto-negotiation modes. It can negotiate with other network devices to determine the operating mode and speed. Thus the suitable operating mode and speed can be worked out automatically and the system configuration and management is greatly streamlined.
- 100Base-FX Multi-mode/Single Mode Ethernet port operates in 100M full-duplex mode. The operating mode can be set to **full** (full-duplex) and **auto** (auto-negotiation) and its speed can be set to **100** (100Mbps) and **auto** (auto-negotiation).

- Gigabit Ethernet port operates in gigabit full-duplex mode. The operating mode can be set to **full** (full-duplex) and **auto** (auto-negotiation) and its speed can be set to **1000** (1000Mbps) and **auto** (auto-negotiation). 1000Base-T Ethernet port operates in 1000M full-duplex, 100M half-duplex/full-duplex, and 10M half-duplex/full-duplex modes.

The configurations of these Ethernet ports are basically the same, which will be described in the following sections.

1.2 Ethernet Port Configuration

Ethernet port configuration includes:

- Enter Ethernet port view
- Enable/Disable Ethernet port
- Set description character string for Ethernet port
- Set duplex attribute for Ethernet port
- Set speed for Ethernet port
- Set cable type for the Ethernet port
- Enable/Disable flow control for Ethernet port
- Set Ethernet port broadcast suppression ratio
- Set link type for Ethernet port
- Add the Ethernet port to specified VLANs
- Set the default VLAN ID for the Ethernet port
- Set loopback detection for the Ethernet port
- Set the time interval of calculating port statistics information

1.2.1 Enter Ethernet port view

Before configuring the Ethernet port, enter Ethernet port view first.

Perform the following configuration in system view.

Table 1-1 Enter Ethernet port view

Operation	Command
Enter Ethernet port view	**interface** { *interface_type interface_num* | *interface_name* }

1.2.2 Enable/Disable Ethernet Port

The following command can be used for disabling or enabling the port. After configuring the related parameters and protocol of the port, you can use the following command to enable the port. If you do not want a port to forward data any more, use the command to disable it.

Perform the following configuration in Ethernet port view.

Table 1-2 Enable/Disable an Ethernet port

Operation	Command
Disable an Ethernet port	**shutdown**
Enable an Ethernet port	**undo shutdown**

By default, the port is enabled.

1.3 Set Description Character String for Ethernet Port

To distinguish the Ethernet ports, you can use the following command to make some necessary descriptions.

Perform the following configuration in Ethernet port view.

Table 1-3 Set description character string for Ethernet port

Operation	Command
Set description character string for Ethernet port.	**description** *text*
Delete the description character string of Ethernet.	**undo description**

By default, the port description is a null character string.

1.3.1 Set Duplex Attribute of the Ethernet Port

To configure a port to send and receive data packets at the same time, set it to full-duplex. To configure a port to either send or receive data packets at a time, set it to half-duplex. If the port has been set to auto-negotiation mode, the local and peer ports will automatically negotiate about the duplex mode.

Perform the following configuration in Ethernet port view.

Table 1-4 Set duplex attribute for Ethernet port

Operation	Command
Set duplex attribute for Ethernet port.	**duplex** { **auto** | **full** | **half** }
Restore the default duplex attribute of Ethernet port.	**undo duplex**

Note that, 100M electrical Ethernet port can operate in full-duplex, half-duplex or auto-negotiation mode, which can be set as per the requirements.

The optical 100M/Gigabit Ethernet ports support full duplex and can be set to operate in **full** (full duplex) or **auto** (auto-negotiation) mode.

The Gigabit electrical Ethernet port can operate in full duplex, half duplex or auto-negotiation mode. When the port operates at 1000Mbps, the duplex mode can be set to **full** (full duplex) or **auto** (auto-negotiation).

The port defaults the **auto** (auto-negotiation) mode.

1.3.2 Set Speed on the Ethernet Port

You can use the following command to set the speed on the Ethernet port. If the speed is set to auto-negotiation mode, the local and peer ports will automatically negotiate about the port speed.

Perform the following configuration in Ethernet port view.

Table 1-5 Set speed on Ethernet port

Operation	Command
Set 100M Ethernet port speed	**speed** { **10** | **100** | **auto** }
Set Gigabit Ethernet port speed	**speed** { **10** | **100** | **1000** | **auto** }
Restore the default speed on Ethernet port	**undo speed**

Note that, the 100M electrical Ethernet port can operate at 10Mbps, 100Mbps or auto-negotiated speed as per different requirements.

100M optical Ethernet port supports 100Mbps and can be configured to operate at **100** (100Mbps) or **auto** (auto-negotiation).

The optical Gigabit Ethernet port supports the 1000Mbps speed and the speed can be set to **1000** (1000Mbps) or **auto** (auto-negotiation).

The electrical Gigabit Ethernet port can operate at 10Mbps, 100Mbps, or 1000Mbps as per different requirements. However in half duplex mode, the port cannot operate at 1000Mbps.

By default, the speed of the port is in **auto** mode.

1.3.3 Set Cable Type for the Ethernet Port

The Ethernet port supports the straight-through and cross-over network cables. The following command can be used for configuring the cable type.

Perform the following configuration in Ethernet port view.

Table 1-6 Set the type of the cable connected to the Ethernet port

Operation	Command
Set the type of the cable connected to the Ethernet port.	**mdi** { **across** | **auto** | **normal** }
Restore the default type of the cable connected to the Ethernet port.	**undo mdi**

Note that, the settings only take effect on 10/100Base-T and 1000Base-T ports.

By default, the cable type is **auto** (auto-recognized).That is, the system can automatically recognize the type of cable connecting to the port.

1.3.4 Enable/Disable Flow Control for Ethernet Port

After enabling flow control in both the local and the peer switch, if congestion occurs in the local switch, the switch will inform its peer to pause packet sending. Once the peer switch receives this message, it will pause packet sending, and vice versa. In this way, packet loss is reduced effectively. The flow control function of the Ethernet port can be enabled or disabled through the following command.

Perform the following configuration in Ethernet port view.

Table 1-7 Enable/Disable Flow Control for Ethernet Port

Operation	Command
Enable Ethernet port flow control	**flow-control**
Disable Ethernet port flow control	**undo flow-control**

By default, Ethernet port flow control is disabled.

1.3.5 Set Ethernet Port Broadcast Suppression Ratio

You can use the following commands to restrict the broadcast traffic. Once the broadcast traffic exceeds the value set by the user, the system will maintain an appropriate broadcast packet ratio by discarding the overflow traffic, so as to suppress broadcast storm, avoid suggestion and ensure the normal service. The parameter is taken the maximum wire speed ratio of the broadcast traffic allowed on the port. The smaller the ratio is, the smaller the broadcast traffic is allowed. If the ratio is 100%, it means not to perform broadcast storm suppression on the port.

Perform the following configuration in Ethernet port view.

Table 1-8 Set Ethernet port broadcast suppression ratio

Operation	Command
Set Ethernet port broadcast suppression ratio	**broadcast-suppression** *ratio*
Restore the default Ethernet port broadcast suppression ratio	**undo broadcast-suppression**

By default, 100% broadcast traffic is allowed to pass through, that is, no broadcast suppression will be performed.

1.3.6 Set link type for Ethernet port

Ethernet port can operate in three different link types, access, hybrid, and trunk types. The access port carries one VLAN only, used for connecting to the user's computer. The trunk port can belong to more than one VLAN and receive/send the packets on multiple VLANs, used for connection between the switches. The hybrid port can also carry more than one VLAN and receive/send the packets on multiple VLANs, used for connecting both the switches and user's computers. The difference between the hybrid port and the trunk port is that the hybrid port allows the packets from multiple VLANs to be sent without tags, but the trunk port only allows the packets from the default VLAN to be sent without tags.

Perform the following configuration in Ethernet port view.

Table 1-9 Set link type for Ethernet port

Operation	Command
Configure the port as access port	**port link-type access**
Configure the port as hybrid port	**port link-type hybrid**
Configure the port as trunk port	**port link-type trunk**
Restore the default link type, that is, the access port.	**undo port link-type**

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.

1.3.7 Add the Ethernet port to Specified VLANs

The following commands are used for adding an Ethernet port to a specified VLAN. The access port can only be added to one VLAN, while the hybrid and trunk ports can be added to multiple VLANs.

Perform the following configuration in Ethernet port view.

Table 1-10 Add the Ethernet port to specified VLANs

Operation	Command
Add the current access port to a specified VLAN	**port access vlan** *vlan_id*
Add the current hybrid port to specified VLANs	**port hybrid vlan** *vlan_id_list* { **tagged** | **untagged** }
Add the current trunk port to specified VLANs	**port trunk permit vlan** { *vlan_id_list* | **all** }
Remove the current access port from to a specified VLAN.	**undo port access vlan**
Remove the current hybrid port from to specified VLANs.	**undo port hybrid vlan** *vlan_id_list*
Remove the current trunk port from specified VLANs.	**undo port trunk permit vlan** { *vlan_id_list* | **all** }

Note that the access port shall be added to an existing VLAN other than VLAN 1. The VLAN to which Hybrid port is added must have been existed. The one to which Trunk port is added cannot be VLAN 1.

After adding the Ethernet port to specified VLANs, the local port can forward packets of these VLANs. The hybrid and trunk ports can be added to multiple VLANs, thereby implementing the VLAN intercommunication between peers. For the hybrid port, you can configure to tag some VLAN packets, based on which the packets can be processed differently.

1.3.8 Set the Default VLAN ID for the Ethernet Port

Since the access port can only be included in one VLAN only, its default VLAN is the one to which it belongs. The hybrid port and the trunk port can be included in several VLANs, it is necessary to configure the default VLAN ID. If the default VLAN ID has been configured, the packets without VLAN Tag will be forwarded to the port that belongs to the default VLAN. When sending the packets with VLAN Tag, if the VLAN ID of the packet is identical to the default VLAN ID of the port, the system will remove VLAN Tag before sending this packet.

Perform the following configuration in Ethernet port view.

Table 1-11 Set the default VLAN ID for the Ethernet port

Operation	Command
Set the default VLAN ID for the hybrid port.	**port hybrid pvid vlan** *vlan_id*
Set the default VLAN ID for the trunk port	**port trunk pvid vlan** *vlan_id*

Operation	Command
Restore the default VLAN ID of the hybrid port to the default value	**undo port hybrid pvid**
Restore the default VLAN ID of the trunk port to the default value	**undo port trunk pvid**

Note that:

- The Trunk port and isolate-user-vlan cannot be configured simultaneously, while the hybrid port and isolate-user-vlan can be thus configured. However, if the default VLAN has been mapped in isolate-user-vlan, you cannot modify the default VLAN ID until the mapping relationship has been removed.
- To guarantee the proper packet transmission, the default VLAN ID of local hybrid port or Trunk port should be identical with that of the hybrid port or Trunk port on the peer switch.

By default, the VLAN of hybrid port and trunk port is VLAN 1 and that of the access port is the VLAN to which it belongs.

1.3.9 Set loopback detection for the Ethernet port

The following commands are used for enabling the port loopback detection and setting detection interval for the external loopback condition of each port. If there is a loopback port found, the switch will put it under control.

Perform the following configuration in corresponding view.

Table 1-12 Set loopback detection for the Ethernet port

Operation	Command
Enable loopback detection on the port (System view/Ethernet port view)	**loopback-detection enable**
Disable loopback detection on the port (System view/Ethernet port view)	**undo loopback-detection enable**
Enable the loopback controlled function of the trunk and hybrid ports (System view/Ethernet port view)	**loopback-detection control enable**
Disable the loopback controlled function of the trunk and hybrid ports (System view/Ethernet port view)	**undo loopback-detection control enable**
Set the external loopback detection interval of the port (System view)	**loopback-detection interval-time** *time*
Restore the default external loopback detection interval of the port (System view)	**undo loopback-detection interval-time**

Operation	Command
Configure that the system performs loopback detection to all VLANs on Trunk and Hybrid ports (Ethernet port view)	**loopback-detection per-vlan enable**
Configure that the system only performs loopback detection to the default VLANs on the port (Ethernet port view)	**undo loopback-detection per-vlan enable**

By default, the port loopback detection is enabled and the detection interval is 30 seconds. The loopback detection controlled function on Trunk or Hybrid port is enabled. The system performs loopback detection to all VLANs on Trunk and Hybrid ports.

1.3.10 Set the Time Interval of Calculating Port Statistics Information

The following commands are used for configuring a time interval. When calculating port statistics information, the switch calculates the average port speed during the time interval.

Perform the following configuration in Ethernet port view.

Table 1-13 Set the time interval of calculating port statistics information

Operation	Command
Set the time interval of calculating port statistics information	**flow-interval** *interval*
Restore the default time interval of calculating port statistics information	**undo flow-interval**

By default, the time interval of calculating port statistics information is 300 seconds.

1.3.11 Port Traffic Threshold Configuration

When port traffic threshold is configured, the system can monitor traffic on the port in a specified interval, and handles the port based on the specified pattern when actual traffic on the port exceeds the threshold. This configuration can effectively prevent port blocking resulted from high traffic and eliminate the effects on the network by malicious or infected users.

You can choose one of the two handling patterns:

1) The system disables the port automatically and sends trap messages.
2) The system sends trap messages only.

I. Port Traffic Threshold Configuration Task

Table 1-14 Port traffic threshold configuration task

Item	Command	Remarks
Enter system view	<Quidway> **system-view**	–
Enter Ethernet port view	[Quidway] **interface** { *interface_type interface_num* | *interface_name* }	–
Configure traffic threshold on the port	[Quidway-EthernetX/X] **flow-constrain** *time-value flow-value* { **bps** | **pps** }	Required
Configure handling pattern when actual traffic on the port exceeds the threshold	[Quidway-EthernetX/X] **flow-constrain method** { **shutdown** | **trap** }	Optional. By default, the system only sends trap messages.

Note:

The prompt character for Ethernet port view may vary with specific configuration.

II. Port Traffic Threshold Configuration Example

1) Configuration requirements

- The traffic threshold on the Ethernet0/1 port is 5000pps and the detection interval is 10 seconds.
- The system disables the port and sends trap messages when actual traffic on the port exceeds the specified threshold.

2) Configuration procedure

Enter system view.

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

Enter Ethernet0/1 port view.

```
[Quidway] interface ethernet0/1
```

Configure the traffic threshold on the Ethernet0/1 port as 5000 pps and the detection interval as 10 seconds.

```
[Quidway-Ethernet0/1] flow-constrain 10 5000 pps
```

Configure the system to disable the port and send trap messages when actual traffic on the port exceeds the threshold.

```
[Quidway-Ethernet0/1] flow-constrain method shutdown
```

1.4 Display and Debug Ethernet Port

After the above configuration, execute **display** command in any view to display the running of the Ethernet port configuration, and to verify the effect of the configuration.

Execute **reset** command in user view to clear the statistics information of the port.

Execute **loopback** command in Ethernet port view to check whether the Ethernet port works normally. In the process of the loopback test, the port cannot forward the packets. The loop test will finish automatically after being executed for a while.

Table 1-15 Display and debug Ethernet port

Operation	Command
Configure to perform loopback test on the Ethernet port.	**loopback** { **external** | **internal** }
Display all the information of the port	**display interface** { *interface_type* | *interface_type interface_num* | *interface_name* }
Display hybrid port or trunk port	**display port** { **hybrid** | **trunk** }
Display the state of loopback detection on the port.	**display loopback-detection**
Clear the statistics information of the port	**reset counters interface** [*interface_type* | *interface_type interface_num* | *interface_name*]

Note that the loopback test cannot be performed on the port disabled by the **shutdown** command. During the loopback test, the system will disable **speed**, **duplex**, **mdi** and **shutdown** operation on the port. Some ports do not support the loopback test. If performing this command in these ports, you will see the system prompt.

1.5 Ethernet Port Configuration Example

I. Networking requirements

Ethernet Switch (Switch A) is connected to the peer (Switch B) via the trunk port Ethernet0/18. The following example configures the default VLAN ID for the trunk port and verifies the **port trunk pvid vlan** command. As a typical application of the **port trunk pvid vlan** command, the trunk port will transmit the packets without tag to the default VLAN.

II. Networking diagram

Figure 1-1 Configure the default VLAN for a trunk port

III. Configuration procedure

The following configurations are used for Switch A. Please configure Switch B in the similar way.

Enter the Ethernet port view of Ethernet0/18.

```
[Quidway] interface ethernet0/18
```

Set the Ethernet0/18 as a trunk port and allows VLAN 2, 6 through 50, and 100 to pass through.

```
[Quidway-Ethernet0/18] port link-type trunk
[Quidway-Ethernet0/18] port trunk permit vlan 2 6 to 50 100
```

Create the VLAN 100.

```
[Quidway] vlan 100
```

Configure the default VLAN ID of Ethernet0/18 as 100.

```
[Quidway-Ethernet0/18] port trunk pvid vlan 100
```

1.6 Ethernet Port Troubleshooting

Fault: Default VLAN ID configuration failed.

Troubleshooting: Take the following steps.

- Execute the **display interface** or **display port** command to check if the port is a trunk port or a hybrid port. If it is neither of them, configure it as a trunk port or a hybrid port.
- Then configure the default VLAN ID.

Chapter 2 Link Aggregation Configuration

2.1 Link Aggregation Overview

The link aggregation means aggregating several ports together to implement the outgoing/incoming payload balance among the member ports and enhance the connection reliability.

An S3026C/S3026G/S3026T/S3026C-PWR Ethernet Switch supports at most six aggregated groups, with each group containing a maximum of eight fixed ports or two extended/uplink ports. The group can start from any port, as long as the ports in it are consecutive.

An S3026E FM/S3026E FS Ethernet Switch supports at most six aggregated groups, with each group containing a maximum of eight ports. The ports of one group located in the same slot must be consecutive. If two slots are involved, the slot numbers should also be consecutive and the first port in the second slot must be added to the group first.

In a link aggregation group, the port with the smallest number serves as the master port, and the others serve as member ports. In one link aggregation group, the link type of the master port and the member ports must be identical. That is, the master port and the member ports should be in Trunk mode together, or be in Access mode together.

2.2 Link Aggregation Configuration

Link aggregation configuration includes:

- Aggregate Ethernet ports

2.2.1 Aggregate Ethernet Ports

The following command can be used for aggregating Ethernet ports or removing a configured link aggregation.

Perform the following configuration in system view.

Table 2-1 Aggregating Ethernet ports

Operation	Command
Aggregate Ethernet ports	**link-aggregation** *port_num1* **to** *port_num2* { **both** | **ingress** }
Remove a configured link aggregation	**undo link-aggregation** { *master_port_num* | **all** }

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.

2.3 Display and Debug Link Aggregation

After the above configuration, execute **display** command in any view to display the running of the link aggregation configuration, and to verify the effect of the configuration.

Table 2-2 Display the information of the link aggregation

Operation	Command
Display the information of the link aggregation	**display link-aggregation** [*master_port_num*]

2.4 Link Aggregation Configuration Example

I. Networking requirements

The following example uses the link aggregation commands to aggregate several ports and implement the outgoing/incoming payload balance among all the member ports. The link aggregation is typically used for Trunk ports. Since the Trunk port allows frames from several VLANs to pass through, the heavy traffic needs balancing among all the ports.

Ethernet Switch (Switch A) is connected to the Ethernet Switch (Switch B) in the upstream via the aggregation of three ports, Ethernet0/1 through Ethernet0/3.

II. Networking diagram

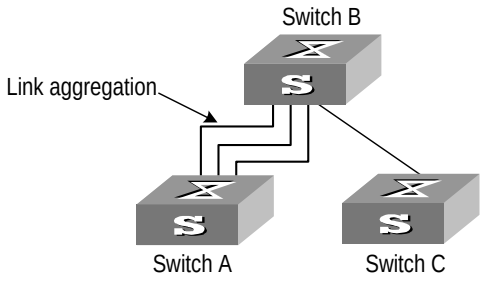


Figure 2-1 Configure link aggregation

III. Configuration procedure

The following configurations are used for Switch A, please configure Switch B in the similar way to activate aggregation.

Aggregate Ethernet0/1 through Ethernet0/3.

```
[Quidway] link-aggregation ethernet0/1 to ethernet0/3 both
```

Display the information of the link aggregation.

```
[Quidway] display link-aggregation ethernet0/1
 Master port: Ethernet0/1
 Other sub-ports:
     Ethernet0/2
     Ethernet0/3
 Mode: both
```

2.5 Ethernet Link Aggregation Troubleshooting

Fault: You might see the prompt of configuration failure when configuring link aggregation.

Troubleshooting:

- Check the input parameter and see whether the starting number of Ethernet port is smaller than the end number. If yes, take the next step.
- Check whether the Ethernet ports that are in the configured range belong to any other existing link aggregations. If not, take the next step.
- Check whether the ports to be aggregated operate in the same speed and full duplex mode. If yes, take the next step.
- Check if there are no more than eight ports in one group.
- If correct, configure the link aggregation again.

HUAWEI

Quidway S3000-EI Series Ethernet Switches
Operation Manual

VLAN

Table of Contents

Chapter 1 VLAN Configuration

1.1 VLAN Overview

Virtual Local Area Network (VLAN) groups the devices of a LAN logically but not physically into segments to implement the virtual workgroups. IEEE issued the IEEE 802.1Q in 1999, which was intended to standardize VLAN implementation solutions.

Through VLAN technology, network managers can logically divide the physical LAN into different broadcast domains. Every VLAN contains a group of workstations with the same demands. The workstations of a VLAN do not have to belong to the same physical LAN segment.

With VLAN technology, the broadcast and unicast traffic within a VLAN will not be forwarded to other VLANs, therefore, it is very helpful in controlling network traffic, saving device investment, simplifying network management and improving security.

1.2 Configure VLAN

To configure a VLAN, first create a VLAN according to the requirements.

Main VLAN configuration includes:

- Enable/Disable VLAN feature
- Create/Delete a VLAN
- Add Ethernet ports to a VLAN
- Set/Delete VLAN description character string

1.2.1 Enable/Disable VLAN Feature

After the VLAN feature is disabled, the packets will be transmitted according to MAC address but not adding VLAN Tag, thereby disabling the function of VLAN isolation. You still may configure IP address of the default management VLAN interface 1, thereby performing remote management such as Telnet and web management.

You can use the following command to enable or disable the VLAN feature on a device.

Perform the following configuration in system view.

Table 1-1 Enable/Disable VLAN feature

Operation	Command
Enable/Disable VLAN feature	**vlan** { **enable** | **disable** }

By default, VLAN feature is enabled on the switch.

Note that you will see error prompt when creating VLAN after VLAN feature is disabled.

1.2.2 Create/Delete a VLAN

You can use the following command to create/delete a VLAN.

Perform the following configurations in system view.

Table 1-2 Create/Delete a VLAN

Operation	Command
Create a VLAN and enter the VLAN view	**vlan** *vlan_id*
Delete the specified VLAN	**undo vlan** { *vlan_id* [**to** *vlan_id*] | **all** }

If the VLAN to be created exists, enter the VLAN view directly. Otherwise, create the VLAN first, and then enter the VLAN view.

vlan_id specifies the VLAN ID. Note that the default VLAN, namely VLAN 1, cannot be deleted.

1.2.3 Add Ethernet Ports to a VLAN

You can use the following command to add the Ethernet ports to a VLAN.

Perform the following configuration in VLAN view.

Table 1-3 Add Ethernet ports to a VLAN

Operation	Command
Add Ethernet ports to a VLAN	**port** *interface_list*
Remove Ethernet ports from a VLAN	**undo port** *interface_list*

By default, the system adds all the ports to a default VLAN, whose ID is 1.

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.

1.2.4 Set/Delete VLAN Description Character String

You can use the following command to set/delete VLAN description character string.

Perform the following configuration in VLAN view.

Table 1-4 Set/Delete VLAN description character string

Operation	Command
Set the description character string for VLAN	**description** *string*
Restore the default description of current VLAN	**undo description**

By default, VLAN description character string is VLAN ID of the VLAN, e.g. VLAN 0001.

1.3 Display and Debug VLAN

After the above configuration, execute **display** command in any view to display the running of the VLAN configuration, and to verify the effect of the configuration.

Table 1-5 Display and debug VLAN

Operation	Command
Display the related information about VLAN	**display vlan**[*vlan_id* | **all** | **static** | **dynamic**]

1.4 VLAN Configuration Example

I. Networking requirements

Create VLAN2 and VLAN3. Add Ethernet port 0/1 and Ethernet port 0/2 to VLAN2 and add Ethernet 0/3 and Ethernet 0/4 to VLAN3.

II. Networking diagram

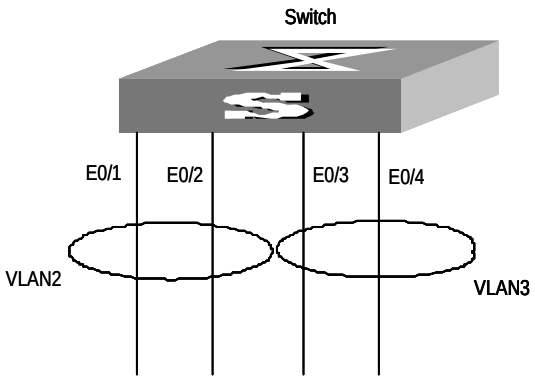


Figure 1-1 VLAN configuration example

III. Configuration procedure

Create VLAN 2 and enters its view.

```
[Quidway] vlan 2
```

Add Ethernet 0/1 and Ethernet 0/2 to VLAN2.

```
[Quidway-vlan2] port ethernet 0/1 to ethernet 0/2
```

Create VLAN 3 and enters its view.

```
[Quidway-vlan2] vlan 3
```

Add Ethernet 0/3 and Ethernet 0/4 to VLAN3.

```
[Quidway-vlan3] port ethernet0/3 to ethernet 0/4
```

Chapter 2 Isolate-User-Vlan Configuration

2.1 Isolate-user-vlan Overview

Isolate-user-vlan is a new feature of the Ethernet Switches launched by Huawei Technologies Co., Ltd., through which can save the VLAN source. isolate-user-vlan adopts the Layer-2 VLAN architecture. (On an Ethernet Switch configure the isolate-user-vlan and Secondary VLAN.) An isolate-user-vlan corresponds to several Secondary VLANs. The isolate-user-vlan includes all the ports and Uplink ports of the corresponding Secondary VLANs. In this way, a upstream switch only needs recognizing the isolate-user-vlan of the downstream switch and ignores those Secondary VLANs, thereby streamlining the configuration and saving the VLAN source. You can use isolate-user-vlan to implement the isolation of the Layer-2 packets through assigning a Secondary VLAN for each user, which only includes the ports and the Uplink ports connected to the user. You can put the ports connected to different users into one Secondary VLAN to implement the Layer-2 packet intercommunication.

2.2 Configure isolate-user-vlan

Isolate-user-vlan configuration includes:

- Configure isolate-user-vlan
- Configure secondary VLAN
- Configure to map isolate-user-vlan to secondary VLAN

The tasks above are required to be configured once you enable the isolate-user-vlan.

2.2.1 Configure isolate-user-vlan

You can use the following commands to create an isolate-user-vlan for an Ethernet switch and add new ports to it.

Create a VLAN in system view, configure it as an isolate-user-vlan and add new ports to it in VLAN view.

Table 2-1 Configure isolate-user-vlan

Operation	Command
Create a VLAN	**vlan** *vlan-id*
Configure the VLAN as isolate-user-vlan	**isolate-user-vlan enable**
Cancel the configuration of VLAN as isolate-user-vlan	**undo isolate-user-vlan enable**
Add new ports to isolate-user-vlan	**port** *interface-list*

An Ethernet switch can have several isolate-user-vlans, each of which can include more than one port. isolate-user-vlan cannot be configured together with the Trunk port. That is to say, you cannot configure a Trunk port on the Ethernet switch already configured with the isolate-user-vlan, and vise versa. In addition, the Uplink port has to be added into the isolate-user-vlan.

2.2.2 Configure Secondary VLAN

You can use the following commands to create a Secondary VLAN and add new ports to it.

Create a secondary VLAN in system view and add new ports to it in VLAN view.

Table 2-2 Configure Secondary VLAN

Operation	Command
Create a Secondary VLAN	**vlan** *vlan-id*
Add new ports to the Secondary VLAN	**port** *interface-list*

You can add more than one port (other than Uplink ports) to a Secondary VLAN.

2.2.3 Configure to Map isolate-user-vlan to Secondary VLAN

You can use the following command to configure the isolate-user-vlan to map the Secondary VLAN.

Perform the following configurations in system view.

Table 2-3 Configure to map isolate-user-vlan to secondary VLAN

Operation	Command
Configure to map isolate-user-vlan to secondary VLAN	**isolate-user-vlan** *isolate-user-vlan_num* **secondary** *secondary_vlan_numlist* [**to** *secondary_vlan_numlist*]
Cancel to map isolate-user-vlan to secondary VLAN	**undo isolate-user-vlan** *isolate-user-vlan_num* [**secondary** *secondary_vlan_numlist* [**to** *secondary_vlan_numlist*]

Note that, before you execute this command, the isolate-user-vlan and Secondary VLAN shall have ports. You can map an isolate-user-vlan to no more than 30 Secondary VLANs.

After the mapping relationship is configured, the system does not allow you to add/remove any ports to/from the isolate-user-vlan or Secondary VLAN or remove a VLAN. You can perform these operations after removing the mapping relationship.

Without the specified **secondary** *secondary_vlan_numlist* parameter, the **undo isolate-user-vlan** command will remove the mapping relationship between the specified isolate-user-vlan and all the Secondary VLANs. Otherwise the relationship between the specified isolate-user-vlan and the specified Secondary VLAN will be removed.

2.2.4 Configure VLAN ID of IGMP packets

You can use the following command to configure VLAN ID of IGMP packets sent to the route interface.

Perform the following configurations in VLAN view.

Table 2-4 Configure VLAN ID of IGMP packets

Operation	Command
Cause IGMP packets to be sent to the route interface with Secondary VLAN ID	**isolate-user-vlan igsp enable**
Restore the default VLAN ID of IGMP packets to be sent to the route interface	**undo isolate-user-vlan igsp enable**

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

2.3 Display and Debug isolate-user-vlan

After the above configuration, execute **display** command in any view to display the running of the isolate-user-vlan configuration, and to verify the effect of the configuration.

Table 2-5 Display and debug isolate-user-vlan

Operation	Command
Display the mapping relationship between the isolate-user-vlan and Secondary VLAN	**display isolate-user-vlan** [*isolate-user-vlan_num*]

2.4 isolate-user-vlan Configuration Example

I. Networking requirements

Switch A is connected to Switch B and Switch C in the downstream. The VLAN5 carried by Switch B is the isolate-user-vlan, including the Uplink Ethernet1/1 and two Secondary VLANs, VLAN2 and VLAN3. VLAN3 includes Ethernet0/1 and VLAN2 includes Ethernet0/2. The VLAN6 carried by Switch C is the isolate-user-vlan including the Uplink Ethernet1/1 and two Secondary VLAN, VLAN3 and VLAN4. VLAN3 includes

Ethernet0/3 and VLAN4 includes Ethernet0/4. Seen from the Switch A, either Switch B or Switch C carries one VLAN, VLAN 5 and VLAN 6 respectively.

II. Networking diagram

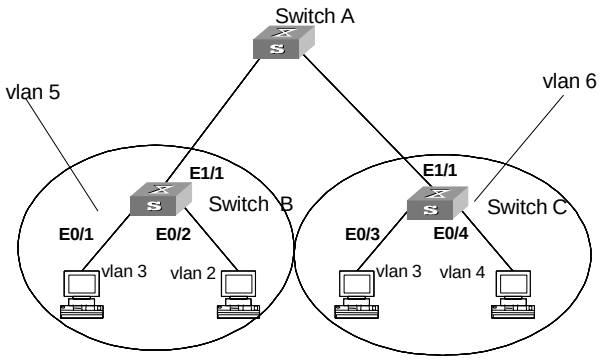


Figure 2-1 isolate-user-vlan configuration example

III. Configuration procedure

Hereafter only listed the configuration procedure of the Switch B and Switch C.

Configure Switch B:

Configure isolate-user-vlan

```
[Quidway] vlan 5
[Quidway-vlan5] isolate-user-vlan enable
[Quidway-vlan5] port ethernet1/1
```

Configure Secondary VLAN

```
[Quidway-vlan5] vlan 3
[Quidway-vlan3] port ethernet0/1
[Quidway-vlan3] vlan 2
[Quidway-vlan2] port ethernet0/2
```

Configure the isolate-user-vlan to Map the Secondary VLAN

```
[Quidway-vlan2] quit
[Quidway] isolate-user-vlan 5 secondary 2 to 3
```

Configure Switch C:

Configure isolate-user-vlan

```
[Quidway] vlan 6
[Quidway-vlan6] isolate-user-vlan enable
[Quidway-vlan6] port ethernet1/1
```

Configure Secondary VLAN

```
[Quidway-vlan6] vlan 3
[Quidway-vlan3] port ethernet0/3
```

```
[Quidway-vlan3] vlan 4
[Quidway-vlan4] port ethernet0/4
```

Configure the isolate-user-vlan to Map the Secondary VLAN

```
[Quidway-vlan4] quit
[Quidway] isolate-user-vlan 6 secondary 3 to 4
```

Chapter 3 GARP/GVRP Configuration

3.1 Configure GARP

3.1.1 GARP Overview

Generic Attribute Registration Protocol (GARP) offers a mechanism that is used by the members in the same switching network to distribute, propagate and register such information as VLAN and multicast addresses.

GARP dose not exist in a switch as an entity. A GARP participant is called GARP application. The main GARP applications at present are GVRP and GMRP. GVRP is described in the GVRP Configuration section and GMRP will be described in Multicast Configuration. When a GARP participant is on a port of the switch, each port corresponds to a GARP participant.

Through GARP mechanism, the configuration information on one GARP member will be advertised rapidly in the whole switching network. GARP member can be a terminal workstation or bridge. A GARP member can notify other members to register or remove its attribute information by sending declarations or withdrawal declarations. It can also register or remove the attribute information of other GARP members according to the received declarations/withdrawal declarations.

GARP members exchange information through sending messages. There mainly are 3 types of GARP messages including Join, Leave, and LeaveAll. When a GARP participant wants to register its attribute information on other switches, it will send Join message outward. When it wants to remove some attribute values from other switches, it will send Leave message. LeaveAll timer will be started at the same time when each GARP participant is enabled and LeaveAll message will be sent upon timeout. Join message and Leave message cooperate to ensure the logout and the re-registration of a message. Through exchanging messages, all the attribute information to be registered can be propagated to all the switches in the same switching network.

The destination MAC addresses of the packets of the GARP participants are specific multicast MAC addresses. A GARP-supporting switch will classify the packets received from the GARP participants and process them with corresponding GARP applications (GVRP or GMRP).

GARP and GMRP are described in details in the IEEE 802.1p standard (which has been added to the IEEE802.1D standard). Quidway Series Ethernet Switches fully support the GARP compliant with the IEEE standards.

Main GARP configuration includes:

- Set GARP timer

Note:

- The value of GARP timer will be used in all the GARP applications, including GVRP and GMRP, running in one switching network.
- In one switching network, the GARP timers on all the switching devices should be set to the same value. Otherwise, GARP application cannot work normally.

3.1.2 Set GARP Timer

GARP timers include Hold timer, Join timer, Leave timer and LeaveAll timer.

The GARP participant sends Join Message regularly when Join timer timeouts so that other GARP participants can register its attribute values.

When the GARP participant wants to remove some attribute values, it will send Leave Message outward. The GARP participant receiving the information will start the Leave timer. If Join Message is not received again before the Leave timer expires, the GARP attribute values will be removed

LeaveAll timer will be started as soon as the GARP participant is enabled. LeaveAll message will be sent upon timeout so that other GARP participants will remove all the attribute values of this participant. Then, Leaveall timer is restarted and a new cycle begins.

When the switch receives some GARP registration information, it will not send Join Message immediately. Instead, it will enable a hold timer and send the Join Message outward upon timeout of the hold timer. In this way, all the VLAN registration information received within the time specified by the Hold timer can be sent in one frame so as to save the bandwidth resource.

Configure Hold timer, Join timer and Leave timer in Ethernet port view. Configure LeaveAll timer in system view.

Table 3-1 Set GARP timer

Operation	Command
Set GARP Hold timer, Join timer and Leave timer	**garp timer** { **hold** | **join** | **leave** } *timer_value*
Set GARP LeaveAll timer	**garp timer leaveall** *timer_value*
Restore the default GARP Hold timer, Join timer and Leave timer settings	**undo garp timer** { **hold** | **join** | **leave** }
Restore the default GARP LeaveAll timer settings.	**undo garp timer leaveall**

Note that, 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. Otherwise, the system will prompt message of error.

By default, Hold timer is 10 centiseconds, Join timer is 20 centiseconds, Leave timer is 60 centiseconds, and LeaveAll timer is 1000 centiseconds.

3.1.3 Display and Debug GARP

After the above configuration, execute **display** command in any view to display the running of GARP configuration, and to verify the effect of the configuration. Execute **reset** command in user view to reset the configuration of GARP. Execute **debugging** command in user view to debug the configuration of GARP.

Table 3-2 Display and debug GARP

Operation	Command
Display GARP statistics information	**display garp statistics** [**interface** *interface-list*]
Display GARP timer	**display garp timer** [**interface** *interface-list*]
Clear GARP statistics information	**reset garp statistics** [**interface** *interface-list*]
Enable GARP event debugging	**debugging garp event**
Disable GARP event debugging	**undo debugging garp event**

3.2 Configure GVRP

3.2.1 GVRP Overview

GARP VLAN Registration Protocol (GVRP) is a GARP application. Based on GARP operating mechanism, GVRP provides maintenance of the dynamic VLAN registration information in the switch and propagates the information to other switches. All the GVRP-supporting switches can receive VLAN registration information from other switches and dynamically update the local VLAN registration information including the active members and through which port those members can be reached. All the GVRP-supporting switches can propagate their local VLAN registration information to other switches so that the VLAN information can be consistent on all GVRP-supporting devices in one switching network. The VLAN registration information propagated by GVRP includes both the local static registration information configured manually and the dynamic registration information from other switches.

GVRP is described in details in the IEEE 802.1Q standard. Quidway Series Ethernet Switches fully support the GARP compliant with the IEEE standards.

Main GVRP configuration includes:

- Enable/Disable global GVRP
- Enable/Disable port GVRP
- Set GVRP registration type

In the above-mentioned configuration tasks, GVRP should be enabled globally before it is enabled on the port. Configuration of GVRP registration type can only take effect after the port GVRP is enabled. Besides, GVRP must be configured on the Trunk port.

3.2.2 Enable/Disable Global GVRP

You can use the following command to enable/disable global GVRP.

Perform the following configurations in system view.

Table 3-3 Enable/Disable global GVRP

Operation	Command
Enable global GVRP	**gvrp**
Disable global GVRP	**undo gvrp**

By default, global GVRP is disabled.

3.2.3 Enable/Disable Port GVRP

You can use the following command to enable/disable the GVRP on a port.

Perform the following configurations in Ethernet port view.

Table 3-4 Enable/Disable port GVRP

Operation	Command
Enable port GVRP	**gvrp**
Disable port GVRP	**undo gvrp**

GVRP should be enabled globally before it is enabled on the port. The GVRP can only be enabled/disabled on Trunk port.

By default, port GVRP is disabled.

3.2.4 Set GVRP Registration Type

The GVRP registration types include Normal, Fixed and Forbidden (see IEEE 802.1Q).

- When an Ethernet port is set to be in Normal registration mode, the dynamic and manual creation, registration and logout of VLAN are allowed on this port.
- When one Trunk port is set as fixed, the system will add the port to the VLAN if a static VLAN is created on the switch and the Trunk port allows the VLAN passing. GVRP will also add this VLAN item to the local GVRP database, one link table for GVRP maintenance. However, GVRP cannot learn dynamic VLAN through this port. The learned dynamic VLAN from other ports of the local switch will not be able to send statements to outside through this port.
- When an Ethernet port is set to be in Forbidden registration mode, all the VLANs except VLAN1 will be logged out and no other VLANs can be created and registered on this port.

Perform the following configurations in Ethernet port view.

Table 3-5 Set GVRP registration type

Operation	Command
Set GVRP registration type	**gvrp registration** { **normal** | **fixed** | **forbidden** }
Restore the default GVRP registration type	**undo gvrp registration**

By default, GVRP registration type is **normal**.

3.2.5 Display and Debug GVRP

After the above configuration, execute **display** command in any view to display the running of GVRP configuration, and to verify the effect of the configuration. Execute **debugging** command in user view to debug the configuration of GVRP.

Table 3-6 Display and debug GVRP

Operation	Command
Display GVRP statistics information	**display gvrp statistics** [**interface** *interface-list*]
Display GVRP global status information	**display gvrp status**
Enable GVRP packet or event debugging	**debugging gvrp** { **packet** | **event**}
Disable GVRP packet or event debugging	**undo debugging gvrp** { **packet** | **event** }

3.2.6 GVRP Configuration Example

I. Networking requirements

To dynamically register and update VLAN information among switches, GVRP needs to be enabled on the switches.

II. Networking diagram

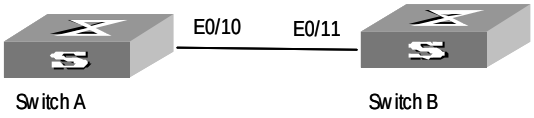


Figure 3-1 GVRP configuration example

III. Configuration procedure

Configure Switch A:

Enable GVRP globally.

```
[Quidway] gvrp
```

Set Ethernet0/10 as a Trunk port and allows all the VLANs to pass through.

```
[Quidway] interface ethernet0/10
[Quidway-Ethernet0/10] port link-type trunk
[Quidway-Ethernet0/10] port trunk permit vlan all
```

Enable GVRP on the Trunk port.

```
[Quidway-Ethernet0/10] gvrp
```

Configure Switch B:

Enable GVRP globally.

```
[Quidway] gvrp
```

Set Ethernet0/11 as a Trunk port and allows all the VLANs to pass through.

```
[Quidway] interface ethernet0/11
[Quidway-Ethernet0/11] port link-type trunk
[Quidway-Ethernet0/11] port trunk permit vlan all
```

Enable GVRP on the Trunk port.

```
[Quidway-Ethernet0/11] gvrp
```

Chapter 4 Voice VLAN Configuration

4.1 Introduction to Voice VLAN

Voice VLAN is specially designed for user's voice flow, and it distributes different port precedence in different cases.

The system uses the source MAC of the traffic traveling through the port to identify the IP Phone data flow. You can either preset an OUI address or adopt the default OUI address as the standard. Here the OUI address refers to that of a vendor.

Voice VLAN can be configured either manually or automatically. In auto mode, the system learns the source MAC address and automatically adds the ports to a Voice VLAN using the untagged packets sent out when IP Phone is powered on; in manual mode, however, you need to add ports to a Voice VLAN manually. Both of the modes forward the tagged packets sent by IP Phone without learning the address.

Since there are multiple types of IP Phones, you must ensure that the mode on a port matches the IP Phone. Please see the following table:

Table 4-1 The corresponding relation between port mode and IP Phone

Voice VLAN Mode	Type of IP Phone	Port Mode
Auto mode	Tagged IP Phone	Access: Do not support
		Trunk: Support, but the default VLAN of the connected port must exist and cannot be the voice VLAN. The default VLAN is allowed to pass the connected port.
		Hybrid: Support, but the default VLAN of the connected port must exist and it is in the tagged VLAN list which is allowed to pass the connected port.
	Untagged IP Phone	Access, Trunk, and Hybrid: Do not support, because the default VLAN of the connected port must be the Voice VLAN, and the connected port belongs to the Voice VLAN, that is, user add the port to the Voice VLAN manually.
Manual mode	Tagged IP Phone	Access: Do not support
		Trunk: Support, but the default VLAN of the connected port must exist and cannot be the voice VLAN. The default VLAN is allowed to pass the connected port.
		Hybrid: Support, but the default VLAN of the connected port must exist and it is in the tagged VLAN list which is allowed to pass the connected port.
	Untagged IP Phone	Access: Support, but the default VLAN of the connected port must be the Voice VLAN.
		Trunk: Support, but the default VLAN of the connected port must be the voice VLAN. The default VLAN is allowed to pass the connected port.
		Hybrid: Support, but the default VLAN of the connected port must be the voice VLAN and it is in the tagged VLAN list which is allowed to pass the connected port.

4.2 Voice VLAN Configuration

The configuration of Voice VLAN includes:

- Enable/disable Voice VLAN features globally
- Enable/disable Voice VLAN features on a port
- Set/remove the OUI address learned by Voice VLAN
- Enable/disable Voice VLAN security mode
- Enable/disable Voice VLAN auto mode
- Set the aging time of Voice VLAN

If you change the status of Voice VLAN security mode, you must first enable Voice VLAN features globally.

4.2.1 Enabling/Disabling Voice VLAN Features

Enable/disable the Voice VLAN in system view.

Table 4-2 Configuring Voice VLAN features

Operation	Command
Enable Voice VLAN features	**voice vlan** *vlan-id* **enable**
Disable Voice VLAN features	**undo voice vlan enable**

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

4.2.2 Enabling/Disabling Voice VLAN Features on a Port

Perform the following configuration in Ethernet port view.

Table 4-3 Configuring Voice VLAN features on a port

Operation	Command
Enable the Voice VLAN features on a port	**voice vlan enable**
Disable the Voice VLAN features on a port	**undo voice vlan enable**

Only the Voice VLAN features in system view and port view are all enabled can the Voice VLAN function on the port run normally.

4.2.3 Setting/Removing the OUI Address Learned by Voice VLAN

Configure OUI addresses which can be learned by Voice VLAN using the following command; otherwise the system uses the default OUI addresses as the standard of IP Phone traffic.

The OUI address system can learn 16 MAC addresses at most. Adding the OUI addresses, you need only input the first three-byte values of the MAC address.

Perform the following configuration in system view.

Table 4-4 Configuring the OUI address learned by Voice VLAN

Operation	command
Set the OUI address learned by Voice VLAN	**voice vlan mac-address** *oui* **mask** *oui-mask* [**description** *string*]
Remove the OUI address learned by Voice VLAN	**undo voice vlan mac-address** *oui*

There are four default OUI addresses after the system starts:

Table 4-5 Default OUI addresses

No.	OUI	Description
1	00e0-bb00-0000	3com phone
2	0003-6b00-0000	Cisco phone
3	00e0-7500-0000	Polycom phone
4	00d0-1e00-0000	Pingtel phone

4.2.4 Enabling/Disabling Voice VLAN Security Mode

In security mode, the system can filter out the traffic whose source MAC is not OUI within the Voice VLAN, while the other VLANs are not influenced. Disabling security mode, the system cannot filter anything.

Perform the following configuration in system view.

Table 4-6 Configuring the Voice VLAN security mode

Operation	Command
Enable Voice VLAN security mode	**voice vlan security enable**
Disable Voice VLAN security mode	**undo voice vlan security enable**

By default, the Voice VLAN security mode is enabled.

4.2.5 Enabling/Disabling Voice VLAN Auto Mode

In auto mode, if you enable Voice VLAN features on a port and there is IP Phone traffic through the port, the system automatically adds the port to the Voice VLAN. But in manual mode, you have to perform the above operation manually.

Perform the following configuration in Ethernet port view.

Table 4-7 Configuring the Voice VLAN auto mode

Operation	Command
Enable the Voice VLAN auto mode	**voice vlan mode auto**
Disable the Voice VLAN auto mode (that is, to enable manual mode)	**undo voice vlan mode auto**

By default, the Voice VLAN auto mode is enabled.

4.2.6 Setting the Aging Time of Voice VLAN

In auto mode, using the follow command, you can set the aging time of Voice VLAN. After the OUI address, the MAC address of IP Phone, is aged on the port, this port enters the aging phase of Voice VLAN. If OUI address is not learned by a port within the aging time, the port is automatically deleted from Voice VLAN. This command does not make sense in manual mode.

Perform the following configuration in system view.

Table 4-8 Configuring the aging time of Voice VLAN

Operation	command
Set the aging time of Voice VLAN	**voice vlan aging** *minutes*
Restore the default aging time	**undo voice vlan aging**

The default aging time is 1440 minutes.

4.3 Displaying and Debugging of Voice VLAN

Finishing the above configuration, use the **display** command in any view to view the configuration and running state of Voice VLAN.

Table 4-9 Displaying Voice VLAN

Operation	Command
Display the status of Voice VLAN	**display voice vlan status**
Display the OUI address supported by the current system	**display voice vlan oui**

4.4 Voice VLAN Configuration Example

I. Networking Requirements

Create VLAN 2 as the Voice VLAN in manual mode and enable its security mode. It is required to set the aging time to 100 minutes, the OUI address to 0011-2200-0000, and configure the port Ethernet1/0/2 as the IP Phone access port. The type of IP Phone is untagged.

II. Network Diagram

None

III. Configuration Steps

```
[Quidway] vlan2
[Quidway-vlan2] port ethernet1/0/2
[Quidway-vlan2] interface ethernet1/0/2
[Quidway-Ethernet1/0/2] voice vlan enable
[Quidway -Ethernet1/0/2] quit
[Quidway] undo voice vlan mode auto
[Quidway] voice vlan mac-address 0011-2200-0000 mask ffff-ff00-0000
description private
[Quidway] voice vlan 2 enable
[Quidway] voice vlan aging 100
```

HUAWEI

Quidway S3000-EI Series Ethernet Switches
Operation Manual

Multicast

Table of Contents

Chapter 1 GMRP Configuration

1.1 GMRP Overview

GMRP (GARP Multicast Registration Protocol), based on GARP, is used for maintaining dynamic multicast registration information of the switch. All the switches supporting GMRP can receive multicast registration information from other switches and dynamically update local multicast registration information. Besides, local multicast registration information can be transmitted to other switches. This information switching mechanism keeps consistency of the multicast information maintained by every GMRP-supporting device in the same switching network.

A host transmits GMRP Join message, if it is interested in joining a multicast group. After receiving the message, the switch adds the port to the multicast group, and broadcasts the message throughout the VLAN, thereby the multicast source in the VLAN knows the multicast member joined. When the multicast source multicasts packets to its group, the switch only forwards the packets to the ports connected to the members, thereby implementing the Layer 2 multicast in VLAN.

The multicast information transmitted by GMRP includes local static multicast registration information configured manually and the multicast registration information dynamically registered by other switches.

1.2 Configure GMRP

The main tasks in GMRP configuration include:

- Enable/Disable GMRP
- Enable/Disable GMRP on the port

In the configuration process, GMRP must be enabled globally before it is enabled on the port.

1.2.1 Enable/Disable GMRP Globally

Perform the following configuration in system view.

Table 1-1 Enable/Disable GMRP globally

Operation	Command
Enable GMRP globally.	**gmrp**
Disable GMRP globally.	**undo gmrp**

By default, GMRP is disabled.

1.2.2 Enable/Disable GMRP on the Port

Perform the following configuration in Ethernet port view.

Table 1-2 Enable/Disable GMRP on the port

Operation	Command
Enable GMRP on the port	**gmrp**
Disable GMRP on the port	**undo gmrp**

GMRP should be enabled globally before enabled on a port.

By default, GMRP is disabled on the port.

1.3 Display and debug GMRP

After the above configuration, execute **display** command in any view to display the running of the GMRP configuration, and to verify the effect of the configuration.

Execute **debugging** command in user view to debug GMRP configuration.

Table 1-3 Display and debug GMRP

Operation	Command
Display GMRP statistics.	**display gmrp statistics** [**interface** *interface_list*]
Display GMRP global status.	**display gmrp status**
Enable GMRP debugging	**debugging gmrp event**
Disable GMRP debugging	**undo debugging gmrp event**

1.4 GMRP Configuration Example

I. Networking requirements

Implement dynamic registration and update of multicast information between switches.

II. Networking diagram

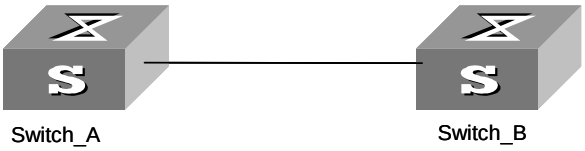


Figure 1-1 GMRP networking

III. Configuration procedure

1) Configure LS_A:

Enable GMRP globally.

```
[Quidway] gmrp
```

Enable GMRP on the port.

```
[Quidway] interface Ethernet 0/1
[Quidway-Ethernet0/1] gmrp
```

2) Configure LS_B:

Enable GMRP globally.

```
[Quidway] gmrp
```

Enable GMRP on the port.

```
[Quidway] interface Ethernet 0/1
[Quidway-Ethernet0/1] gmrp
```

Chapter 2 IGMP Snooping Configuration

2.1 IGMP Snooping Overview

2.1.1 IGMP Snooping Principle

IGMP Snooping (Internet Group Management Protocol Snooping) is a multicast control mechanism running on the Layer 2 Ethernet switch and it is used for multicast group management and control.

IGMP Snooping runs on the link layer. When receiving the IGMP messages transmitted between the host and router, the Layer 2 Ethernet switch uses IGMP Snooping to analyze the information carried in the IGMP messages. If the switch hears IGMP host report message from an IGMP host, it will add the host to the corresponding multicast table. If the switch hears IGMP leave message from an IGMP host, it will remove the host from the corresponding multicast table. The switch continuously listens to the IGMP messages to create and maintain MAC multicast address table on Layer 2. And then it can forward the multicast packets transmitted from the upstream router according to the MAC multicast address table.

When IGMP Snooping is disabled, the packets are multicast on Layer 2. See the following figure:

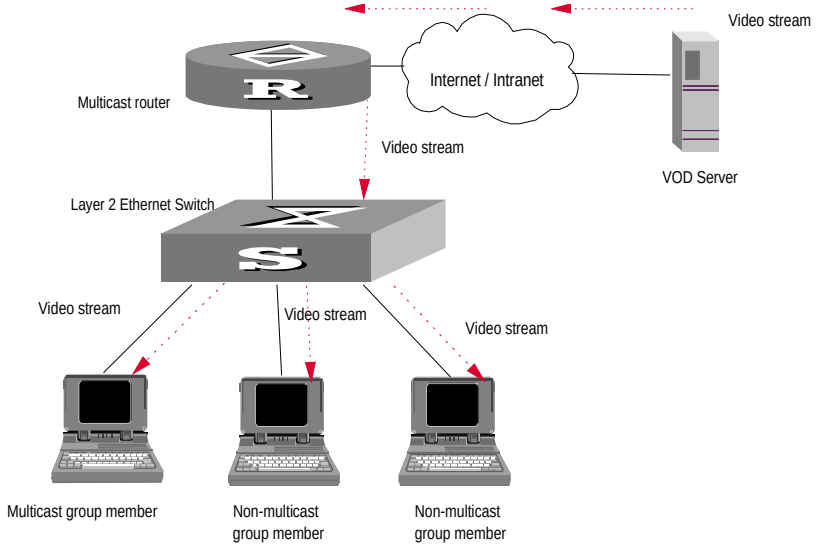


Figure 2-1 Multicast packet transmission without IGMP Snooping

When IGMP Snooping runs, the packets are not broadcast on Layer 2. See the following figure:

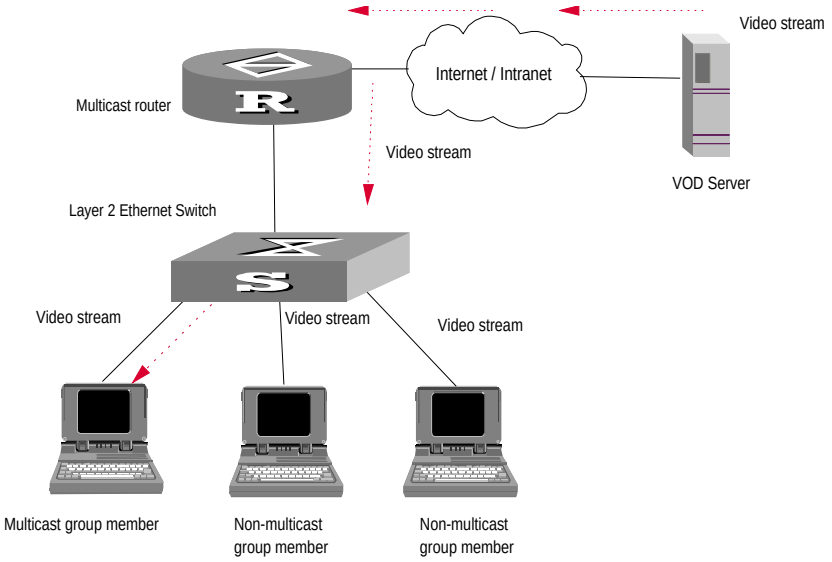


Figure 2-2 Multicast packet transmission when IGMP Snooping runs

2.1.2 Implement IGMP Snooping

I. Related concepts of IGMP Snooping

To facilitate the description, this section first introduces some related switch concepts of IGMP Snooping:

- Router Port: The port of the switch, directly connected to the multicast router.
- Multicast member port: The port connected to the multicast member. The multicast member refers to a host joined a multicast group.
- MAC multicast group: The multicast group is identified with MAC multicast address and maintained by the Ethernet switch.
- Router port aging time: Time set on the router port aging timer. If the switch has not received any IGMP general query message before the timer times out, it considers the port no longer as a router port.
- Multicast group member port aging time: When a port joins an IP multicast group, the aging timer of the port will begin timing. The multicast group member port aging time is set on this aging timer. If the switch has not received any IGMP report message before the timer times out, it transmits IGMP specific query message to the port.
- Maximum response time: When the switch transmits IGMP specific query message to the multicast member port, the Ethernet switch starts a response timer, which times before the response to the query. If the switch has not received any IGMP report message before the timer times out, it will remove the port from the multicast member ports

II. Implement Layer 2 multicast with IGMP Snooping

The Ethernet switch runs IGMP Snooping to listen to the IGMP messages and map the host and its ports to the corresponding multicast group address. To implement IGMP Snooping, the Layer 2 Ethernet switch processes different IGMP messages in the way illustrated in the figure below:

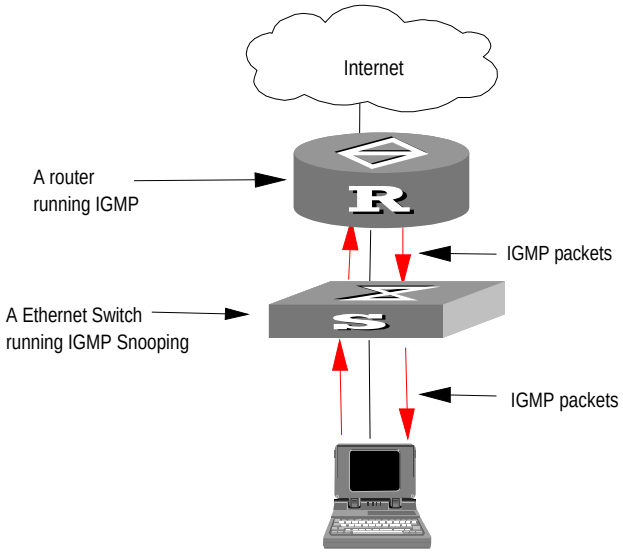


Figure 2-3 Implement IGMP Snooping

1) IGMP general query message: Transmitted by the multicast router to the multicast group members to query which multicast group contains member. When an IGMP general query message arrives at a router port, the Ethernet switch will reset the aging timer of the port. When a port other than a router port receives the IGMP general query message, the Ethernet switch will notify the multicast router that a port is ready to join a multicast group and starts the aging timer for the port.
2) IGMP specific query message: Transmitted from the multicast router to the multicast members and used for querying if a specific group contains any member. When received IGMP specific query message, the switch only transmits the specific query message to the IP multicast group which is queried.
3) IGMP report message: Transmitted from the host to the multicast router and used for applying to a multicast group or responding to the IGMP query message. When received the IGMP report message, the switch checks if the MAC multicast group, corresponding to the IP multicast group the packet is ready to join exists. If the corresponding MAC multicast group does not exist, the switch only notifies the router that a member is ready to join a multicast group, creates a new MAC multicast group, adds the port received the message to the group, starts the port aging timer, and then adds all the router ports in the native VLAN of the port into the MAC multicast forwarding table, and meanwhile creates an IP multicast group and adds the port received the report message to it. If the corresponding MAC

multicast group exists but does not contains the port received the report message, the switch adds the port into the multicast group and starts the port aging timer. And then the switch checks if the corresponding IP multicast group exists. If it does not exist, the switch creates a new IP multicast group and adds the port received the report message to it. If it exists, the switch adds the port to it. If the MAC multicast group corresponding to the message exists and contains the port received the message, the switch will only reset the aging timer of the port.

4) IGMP leave message: Transmitted from the multicast group member to the multicast router to notify that a router host left the multicast group. When received a leave message of an IP multicast group, the Ethernet switch transmits the specific query message concerning that group to the port received the message, in order to check if the host still has some other member of this group and meanwhile starts a maximum response timer. If the switch has not receive any report message from the multicast group, the port will be removed from the corresponding MAC multicast group. If the MAC multicast group does not have any member, the switch will notify the multicast router to remove it from the multicast tree.

2.2 Configure IGMP Snooping

The main IGMP Snooping configuration includes:

- Enable/disable IGMP Snooping
- Configure the aging time of router port
- Configure maximum response time
- Configure the aging time of multicast group member port
- Enabling/Disabling the function of fast removing a port from a multicast group
- Setting the maximum number of multicast groups permited on a port
- Configuring IGMP Snooping Filter

Among the above configuration tasks, enabling IGMP Snooping is required, while others are optional for your requirements.

2.2.1 Enable/Disable IGMP Snooping

You can use the following commands to enable/disable IGMP Snooping to control whether MAC multicast forwarding table is created and maintained on Layer 2.

Perform the following configuration in system view.

Table 2-1 Enable/Disable IGMP Snooping

Operation	Command
Enable/disable IGMP Snooping	**igmp-snooping** { **enable** | **disable** }
Restore the default setting	**undo igmp-snooping**

IGMP Snooping and GMRP cannot run at the same time. You can check if GMRP is running, using the **display gmrp status** command, in any view, before enabling IGMP Snooping.

By default, IGMP Snooping is disabled.

2.2.2 Configure Router Port Aging Time

This task is to manually configure the router port aging time. If the switch has not received any general query message from the router before the router port is aged, it will remove the port from all the MAC multicast group.

Perform the following configuration in system view.

Table 2-2 Configure router port aging time

Operation	Command
Configure router port aging time	**igmp-snooping router-aging-time** *seconds*
Restore the default aging time	**undo igmp-snooping router-aging-time**

By default, the port aging time is 260s.

2.2.3 Configure Maximum Response Time

This task is to manually configure the maximum response time. If the Ethernet switch receives no report message from a port in the maximum response time, it will remove the port from the multicast group.

Perform the following configuration in system view.

Table 2-3 Configure the maximum response time

Operation	Command
Configure the maximum response time	**igmp-snooping max-response-time** *seconds*
Restore the default setting	**undo igmp-snooping max-response-time**

By default, the maximum response time is 10 seconds.

2.2.4 Configure Aging Time of Multicast Group Member

This task is to manually set the aging time of the multicast group member port. If the switch receives no multicast group report message during the member port aging time, it will transmit the specific query message to that port and starts a maximum response timer.

Perform the following configuration in system view.

Table 2-4 Configure aging time of the multicast member

Operation	Command
Configure aging time of the multicast member	**igmp-snooping host-aging-time** *seconds*
Restore the default setting	**undo igmp-snooping host-aging-time**

By default, the aging time of the multicast member is 260 seconds.

2.2.5 Enabling/Disabling the function of fast removing a port from a multicast group

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 form the group. By configuring the follwing 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.

Perform the following configuration in Ethernet port view.

Table 2-5 Enabling/Disabling the function of fast removing a port from a multicast group

Operation	Command
Enable the function of fast removing a port from a multicast group	**igmp-snooping fast-leave**
Disable the function of fast removing a port from a multicast group	**undo igmp-snooping fast-leave**

By default, the fast remove function is disabled.

Note:

- 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.

2.2.6 Setting the maximum number of multicast groups permited on a port

Perform the following configuration in Ethernet port view.

Table 2-6 Setting the maximum number of multicast groups permited on a port

Operation	Command
Set the maximum number of multicast groups permited on a port	**igmp-snooping group-limit** *limit*
Restore the default value	**undo igmp-snooping group-limit**

By default, the maximum number of multicast groups permited on a port is 1000.

2.2.7 Configuring IGMP Snooping Filter

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.

Perform the following configuration in Ethernet port view.

Table 2-7 Configuring IGMP Snooping Filter

Operation	Command
Configure the filtering on the port	**igmp-snooping group-policy** *acl_num* **vlan** *vlan_id*
Cancel the filtering configured on the port	**undo igmp-snooping group-policy** *acl_num* **vlan** *vlan_id*

By default, no filtering configured on the switch.

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, s o 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.

2.2.8 Multicast Source Port Suppression Configuration

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.

I. Enabling/Disabling Multicast Source Port Suppression

Perform the following configuration in system view or Ethernet port view.

Table 2-8 Enable/disable multicast source port suppression function

Operation	Command
Enable multicast source port suppression	**multicast-source-deny** [**interface** *interface-list*]
Disable multicast source port suppression	**undo multicast-source-deny** [**interface** *interface-list*]

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

- In system view, if the interface-list parameter is not specified, it means that to enable this function globally; that is, to enable this function on all ports of the switch; 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

II. Displaying and Debugging Multicast Source Port Suppression

After the above configuration, perform the **display** command in any view, you can view the running state of multicast source port suppression, and check the configuration result.

Table 2-9 Display and debug multicast source port suppression

Operation	Command
Display statistics about multicast source port suppression	**display multicast-source-deny** [**interface** { *interface_type* [*interface_number*] | *interface_name* **}**]

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.

2.3 Display and debug IGMP Snooping

After the above configuration, execute **display** command in any view to display the running of the IGMP Snooping configuration, and to verify the effect of the configuration. Execute **debugging** command in user view to debug IGMP Snooping configuration.

Table 2-10 Display and debug IGMP Snooping

Operation	Command
Display the information about current IGMP Snooping configuration	**display igmp-snooping configuration**
Display IGMP Snooping statistics of received and sent messages	**display igmp-snooping statistics**
Display IP/MAC multicast group information in the VLAN	**display igmp-snooping group** [**vlan** *vlanid*]
Enable/disable IGMP Snooping debugging (abnormal, group, packet, timer).	**debugging igmp-snooping** { **all** | **abnormal** | **group** | **packet** | **timers** }
Disable IGMP Snooping debugging (abnormal, group, packet, timer).	**undo debugging igmp-snooping** { **all** | **abnormal** | **group** | **packet** | **timers** }

2.4 IGMP Snooping Configuration Example

2.4.1 Enable IGMP Snooping

I. Networking requirements

To implement IGMP Snooping on the switch, first enable it. The switch is connected with the router via the router port, and with user PC through the non-router ports.

II. Networking diagram

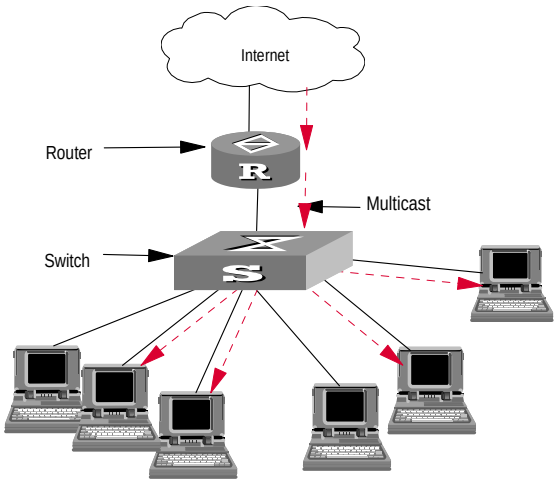


Figure 2-4 IGMP Snooping configuration networking

III. Configuration procedure

Display the status of GMRP.

```
<Quidway> display gmrp status
```

Display the current status of IGMP Snooping when GMRP is disabled.

```
<Quidway> display igmp-snooping configuration
```

Enable IGMP Snooping if it is disabled.

```
[Quidway] igmp-snooping enable
```

2.5 Troubleshoot IGMP Snooping

Fault: Multicast function cannot be implemented on the switch.

Troubleshooting:

1) IGMP Snooping is disabled.

- Input the **display current-configuration** command to display the status of IGMP Snooping.
- If the switch disabled IGMP Snooping, you can input **igmp-snooping enable** in the system view to enable IGMP Snooping.

2) Multicast forwarding table set up by IGMP Snooping is wrong.

- Input the **display igmp-snooping group** command to display if the multicast group is the expected one.
- If the multicast group created by IGMP Snooping is not correct, turn to professional maintenance personnel for help.
- Continue with diagnosis 3 if the second step is completed.

3) Multicast forwarding table set up on the bottom layer is wrong.

- Enable IGMP Snooping group in user view and then input the command **display igmp-snooping group** to check if MAC multicast forwarding table in the bottom layer and that created by IGMP Snooping is consistent. You may also input the **display mac vlan** command in any view to check if MAC multicast forwarding table under vlanid in the bottom layer and that created by IGMP Snooping is consistent.
- If they are not consistent, please contact the maintenance personnel for help.

Chapter 3 Unknown Multicast Dropping Configuration

3.1 Introduction to Unknown Multicast Dropping

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.

3.2 Unknown Multicast Dropping Configuration

Unknown Multicast Dropping Configuration includes:

- Enable unknown multicast dropping function

3.2.1 Enable Unknown Multicast Dropping

Perform the following configuration in system view.

Table 3-1 Enable the unknown multicast dropping function

Operation	Command
Enable the unknown multicast dropping function	**unknown-multicast drop enable**
Disable the unknown multicast dropping function	**undo unknown-multicast drop enable**

By default, the unknown-multicast drop function is disabled.

Chapter 4 Adding Multicast MAC Address Configuration

4.1 Introduction

In Layer 2 multicast, you can not only dynamically create multicast forwarding entries using the Layer 2 multicast protocol, but also set manually the multicast MAC address and bind multicast entries to ports.

Generally, the packet is not broadcasted among the VLAN if its multicast address is not registered on the local host. You can enable the broadcast, however, by configuring a multicast static MAC address entry. Then the switch changes from dynamic multicast learning to static multicast learning and saves the time originally to handle multicast packets.

If you configure the switch not to forward unknown multicast packets (enabling the unknown multicast blocked function), the switch cannot forward some specific multicast packets (such as VRRP packets). You can enable to forward these types of packets by adding multicast MAC address entries.

4.2 Adding Multicast MAC Address Entries

Follow these steps to add multicast MAC address entries:

Table 4-1 Add multicast MAC address entries

Operation	Command	Remarks
Enter system view	**system-view**	-
Add multicast MAC address entries	**mac-address multicast** *mac-address* **interface** *interface-list* **vlan** *vlan_id*	Mandatory

Use the **undo** command to remove your configuration.

- If the multicast MAC address entry you intend to add has existed, the system gives the prompt information.
- After you manually add a multicast MAC address, the switch cannot learn it using IGMP snooping. The command can only remove the multicast MAC address entries manually added, but not those learned by the switch.
- To add a port to the multicast MAC address entry which is manually added, you need first delete the entry and create it again, and then add the specified port as the forwarding port of the entry.

Chapter 5 Multicast VLAN Configuration

5.1 Introduction to Multicast VLAN

Generally, when users in different virtual LANs (VLANs) order a multicast stream, each of these VLANs copies the same multicast stream to itself. In this method, a great deal of bandwidth is wasted.

Multicast VLAN is used to solve this problem. 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.

5.2 Multicast VLAN Configuration

5.2.1 Configuration Tasks

Though multicast VLAN is mainly implemented at layer 2 switching, you must configure it on both layer 2 and 3 switches.

The following table describes the multicast VLAN configuration tasks

Table 5-1 Multicast VLAN configuration tasks on layer 3 switch

Item	Command	Description
Entering the system view	**system-view**	-
Creating a VLAN	**vlan** *vlan-id*	-
Entering the VLAN view	**interface Vlan-interface** *vlan-id*	-
Enabling IGMP	**igmp enable**	Required
Quitting the VLAN view	**service-type multicast**	Required
Quitting the VLAN view	**quit**	-
Entering the Ethernet port view connected with the layer 2 switch	**interface** *interface_type interface_num*	*interface_type*: port type *interface_num*: port number
Defining the type of the port to trunk or hybrid	**port link-type** { **trunk** | **hybrid** }	Required

Item	Command	Description
Setting the default VLAN ID of the Ethernet port	**port hybrid vlan** *vlan_id_list* { **tagged** | **untagged** }	Required
	port trunk pvid vlan *vlan_id*	

Table 5-2 Multicast VLAN configuration tasks on layer 2 switch

Item	Command	Description
Entering the system view	**system-view**	-
Enabling IGMP Snooping function in system view	**igmp-snooping enable**	Required
Entering a VLAN view	**vlan** *x*	*x* is a VLAN ID.
Enabling the IGMP Snooping function in the VLAN view	**igmp-snooping enable**	Required
Enabling the multicast VLAN function	**service-type multicast**	Required
Quitting the VLAN view	**quit**	-
Entering the Ethernet port view connected with the layer 3 switch	**interface** *interface_type interface_num*	*interface_type*: port type *interface_num*: port number
Defining the type of the port to trunk or hybrid	**port link-type** { **trunk | hybrid** }	Required
Setting the default VLAN ID of the Ethernet port	**port hybrid vlan** *vlan_id_list* { **tagged** | **untagged** }	-
	port trunk pvid vlan *vlan_id*	
Entering the Ethernet port view connected with the user	**interface** *interface_type interface_num*	*interface_type*: port type *interface_num*: port number
Defining the type of the port to hybrid	**port link-type hybrid**	Required
Specifying VLANs for the port	**port hybrid vlan** *vlan_id_list* { **tagged** | **untagged** }	Required

To cancel the configurations, use the corresponding **undo** commands.

Note:

- The isolate vlan cannot be set to a multicast VLAN.
- Only one multicast VLAN can be specified for a port.
- The type of the ports connected with user terminals can only be hybrid.

5.3 Multicast VLAN Configuration Example

I. Network requirements

The devices and requirements are as follows:

Device	Role	Description
Switch A	Layer 3 switch	The IP address of the VLAN 20 interface is 168.10.1.1; The port E1/0/1 belongs to VLAN 20 and is connected with the workstation. VLAN 10 acts as a multicast VLAN. The port E1/0/10 is connected with switch B.
Switch B	Layer 2 switch	VLAN 2 includes the port E1/0/1, which is connected with PC1; the VLAN 3 includes the port E1/0/2, which is connected with PC2. The port E1/0/10 is connected with switch A.
PC 1	User 1	PC1 is connected with switch B through port E1/0/1.
PC 2	User 2	PC2 is connected with switch B through port E1/0/2.

perform the following multicast VLAN configuration to allow users in VLAN 2 and VLAN 3 to receive multicast streams through the multicast VLAN.

II. Network diagram

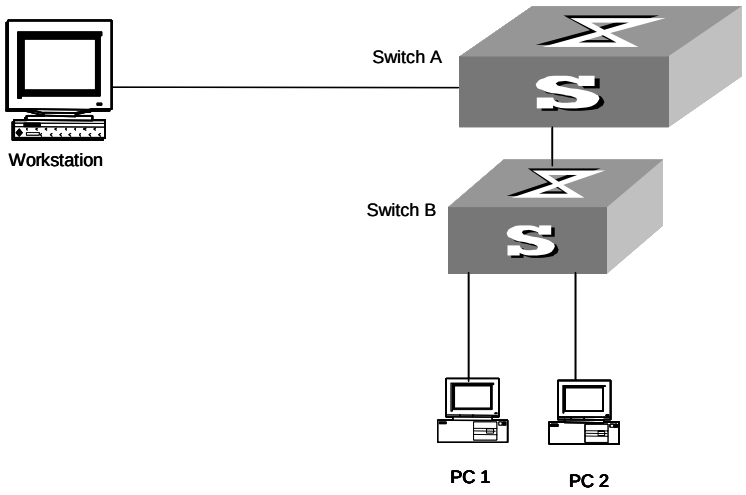


Figure 5-1 Network diagram for multicast VLAN

III. Configuration procedure

This procedure supposes that the IP addresses have been configured and the devices are properly connected.

1) Configure switch A as follows:

Configure the IP address of the VLAN 20 interface to 168.10.1.1 and enable the PIM DM protocol.

```
<Switch A> system-view
[Switch A] multicast routing-enable
[Switch A] vlan 20
[Switch A-vlan20] interface vlan-interface 20
[Switch A-Vlan-interface20] ip address 168.10.1.1 255.255.255.0
[Switch A-Vlan-interface20] pim dm
[Switch A-Vlan-interface20] quit
```

Configure VLAN 10.

```
[Switch A] vlan 10
[Switch A-vlan10] quit
```

Define the type of the Ethernet 1/0/10 port to hybrid. Then join the port to VLAN 2, 3 and 10 with the **tagged** option for the port to carry VLAN tag when transmitting packets of these VLANs.

```
[Switch A] interface Ethernet 1/0/10
[Switch A-Ethernet 1/0/10] port link-type hybrid
[Switch A-Ethernet 1/0/10] port hybrid vlan 2 3 10 tagged
[Switch A-Ethernet 1/0/10] quit
```

Enable the PIM DM protocol and the IGMP function on the VLAN 10 interface.

```
[Switch A] multicast routing-enable
[Switch A] interface Vlan-interface 10
[Switch A-Vlan-interface10] pim dm
[Switch A-Vlan-interface10] igmp enable
```

2) Configure switch B as follows:

Enable IGMP Snooping

```
<Switch B> system-view
[Switch B] igmp-snooping enable
```

Set VLAN 10 to multicast VLAN and enable IGMP Snooping.

```
[Switch B] vlan 10
[Switch B-vlan10] service-type multicast
[Switch B-vlan10] igmp-snooping enable
[Switch B-vlan10] quit
```

Define the type of the Ethernet 1/0/10 port to hybrid. Then join the port to VLAN 2, 3 and 10 with the **tagged** option for the port to carry VLAN tag when transmitting packets of these VLANs.

```
[Switch B] interface Ethernet 1/0/10
[Switch B-Ethernet 1/0/10] port link-type hybrid
[Switch B-Ethernet 1/0/10] port hybrid vlan 2 3 10 tagged
[Switch B-Ethernet 1/0/10] quit
```

Define the type of the Ethernet 1/0/1 port to hybrid. Then join the port to VLAN 2 and 10 with the **untagged** option for the port to transmit packets of these VLANs without carrying VLAN tag. Finally set the default VLAN ID of the port to VLAN 2.

```
[Switch B] interface Ethernet 1/0/1
[Switch B-Ethernet 1/0/1] port link-type hybrid
[Switch B-Ethernet 1/0/1] port hybrid vlan 2 10 untagged
[Switch B-Ethernet 1/0/1] port hybrid pvid vlan 2
[Switch B-Ethernet 1/0/1] quit
```

Define the type of the Ethernet 1/0/2 port to hybrid. Then join the port to VLAN 3 and 10 with the **untagged** option for the port to transmit packets of these VLANs without carrying VLAN tag. Finally set the VLAN ID of the port to VLAN 3.

```
[Switch B] interface Ethernet 1/0/1
[Switch B-Ethernet 1/0/2] port link-type hybrid
[Switch B-Ethernet 1/0/2] port hybrid vlan 3 10 untagged
[Switch B-Ethernet 1/0/2] port hybrid pvid vlan 3
[Switch B-Ethernet 1/0/2] quit
```

HUAWEI

Quidway S3000-EI Series Ethernet Switches
Operation Manual

QoS/ACL

Table of Contents

Chapter 1 ACL Configuration

1.1 Brief Introduction to ACL

1.1.1 ACL Overview

A series of matching rules are required for the network devices to identify the packets to be filtered. After identifying the packets, the switch can permit or deny them to pass through according to the defined policy. Access Control List (ACL) is used to implement such functions.

ACL classifies the data packets with a series of matching rules, including source address, destination address and port number, etc. The switch verifies the data packets with the rules in ACL and determines to forward or discard them.

The data packet matching rules defined by ACL can also be called in some other cases requiring traffic classification, such as defining traffic classification for QoS.

An access control rule includes several statements. Different statements specify different ranges of packets. When matching a data packet with the access control rule, the issue of match-order arises.

I. Case of filtering or classifying data transmitted by the hardware

ACL can be used to filter or classify the data transmitted by the hardware of switch. In this case, the match order of ACL's sub-rules is determined by the switch hardware. The match order defined by the user can't be effective.

Due 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

Switch	Hardware match order of ACL's sub-rule
S3000-EI series	An ACL is configured with multiple sub-rules. The latest sub-rule will be matched first.

The case includes: ACL cited by QoS function, ACL used for filter the packet transmitted by the hardware. etc.

II. Case of filtering or classifying data transmitted by the software

ACL can be used to filter or classify the data treated by the software of switch. In this case, the match order of ACL's sub-rules can be determined by the user. There are two match-orders: **config** (by following the user-defined configuration order when matching the rule) and **auto** (according to the system sorting automatically when matching the

rule, i.e. in depth-first order). Once the user specifies the match-order of an access control rule, he cannot modify it later, unless he deletes all the content and specifies the match-order again.

The case includes: ACL cited by route policy function, ACL used for control logon user, etc.

Note:

The depth-first principle is to put the statement specifying the smallest range of packets on the top of the list. This can be implemented through comparing the wildcards of the addresses. The smaller the wildcard is, the less hosts it can specify. For example, 129.102.1.1 0.0.0.0 specifies a host, while 129.102.1.1 0.0.255.255 specifies a network segment, 129.102.0.1 through 129.102.255.255. Obviously, the former one is listed ahead in the access control list.

The specific standard is as follows.

For basic access control list statements, comparing the source address wildcards directly. If the wildcards are same, follow the configuration sequence.

For the access control list based on the interface filter, the rule that is configured with **any** is listed in the end, while others follow the configuration sequence.

For the advanced access control list, comparing the source address wildcards first. If they are the same, then comparing the destination address wildcards. For the same destination address wildcards, comparing the ranges of port number, the one with smaller range is listed ahead. If the port numbers are in the same range, follow the configuration sequence.

1.1.2 ACL Supported by the Ethernet Switch

For Ethernet Switch, ACLs are divided into the following categories:

- Numbered basic ACL.
- Named basic ACL.
- Numbered advanced ACL.
- Named advanced ACL.
- Numbered Layer-2 ACL.
- Named Layer-2 ACL.
- Numbered user-defined ACL.
- Named user-defined ACL.

The table below lists the limits to the numbers of different ACL on a switch.

Table 1-2 Quantitative limitation to ACL

Item	Value range
Numbered basic ACL.	2000 to 2999
Numbered advanced ACL.	3000 to 3999
Numbered Layer-2 ACL.	4000 to 4999
Numbered user-defined ACL.	5000 to 5999
Named basic ACL.	-
Named advanced ACL.	-
Named Layer-2 ACL.	-
Named user-defined ACL.	-
The sub items of an ACL	0 to 127

1.2 Configuring ACL

ACL configuration includes:

- Configuring the time range
- Defining ACL
- Activating ACL

The above three steps had better be taken in sequence. Configure time range first and then define ACL (using the defined time range in the definition), followed activating ACL to validate it.

1.2.1 Configuring the Time-Range

The process of configuring a time-range includes the steps of configuring the hour-minute range, date ranges and period range. The hour-minute range is expressed in the units of minute, hour. Date range is expressed in the units of minute, hour, date, month and year. The periodic time range is expressed in the day of the week.

You can use the following command to set the time range by performing the following configuration in the system view.

Table 1-3 Setting the absolute time range

Operation	Command
Set the absolute time range	**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*] }

Operation	Command
Delete the absolute time range	**undo time-range** *time-name* [*start-time* **to** *end-time days-of-the-week* | **from** *start-time start-date*]* [**to** *end-time end-date*]

When the start-time and end-time are not configured, it will be all the time for one day. The end time shall be later than the start time.

When *end-time end-date* is not configured, it will be all the time from now to the date which can be displayed by the system. The end time shall be later than the start time.

1.2.2 Defining ACL

Huawei Switches support several kinds of ACLs. Here we will introduce how to define these ACLs.

Defining ACL by following the steps below:

1) enter the corresponding ACL view
2) add a rule to the ACL

You can add multiple rules to one ACL.

Note:

- If a specific time rang is not defined, the ACL will always function after activated.
- During the process of defining the ACL, you can use the **rule** command for several times to define multiple rules for an ACL.
- If ACL is used for filter or classify the data transmitted by the hardware of switch, the match order defined in the **acl** command will not be effective. If ACL is used for filter or classify the data treated by the software of switch, the match order of ACL's sub-rules will be effective. Besides, once the user specifies the match-order of an ACL rule, he cannot modify it later.
- The default matching-order of ACL is **config**, i.e. following the order as that configured by the user.

I. Defining the basic ACL

The rules of the basic ACL are defined on the basis of the Layer-3 source IP address to analyze the data packets.

You can use the following command to define basic ACL.

Perform the following configuration in corresponding view.

Table 1-4 Defining the basic ACL

Operation	Command
Enter basic ACL view(from system view)	**acl** { **number** *acl-number* | **name** *acl-name* **basic** } [**match-order** { **config** | **auto** }]
add a sub-item to the ACL(from basic ACL view)	**rule** [*rule-id*] { **permit** | **deny** } [**source** { *source-addr wildcard* | **any** } | **fragment** | **time-range** *name*]*
delete a sub-item from the ACL(from basic ACL view)	**undo rule** *rule-id* [**source** | **fragment** | **time-range**]*
Delete one ACL or all the ACL(from system view)	**undo acl** { **number** *acl-number* | **name** *acl-name* | **all** }

II. Defining the advanced ACL

The rules of the classification for advanced ACL are defined on the basis of the attributes such as source and destination IP address, the TCP or UDP port number in use and packet priority to process the data packets. The advanced ACL supports the analyses of three kinds of packet priorities, ToS (Type of Service), IP and DSCP priorities.

You can use the following command to define advanced ACL.

Perform the following configuration in corresponding view.

Table 1-5 Defining the advanced ACL

Operation	Command
Enter advanced ACL view(from system view)	**acl** { **number** *acl-number* | **name** *acl-name* **advanced** } [**match-order** { **config** | **auto** }]
Add a sub-item to the ACL(from advanced ACL view)	**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*]
Delete a sub-item from the ACL(from advanced ACL view)	**undo rule** *rule-id* [**destination** | **destination-port** | **dscp** | **fragment** | **icmp-type** | **precedence** | **source** | **source-port** | **time-range** | **tos**]*
Delete one ACL or all the ACL(from system view)	**undo acl** { **number** *acl-number* **| name** *acl-name* | **all** }

The advanced ACL is identified with the numbers ranging from 3000 to 3999.

Note that, the *port1* and *port2* in the above command specify the TCP or UDP ports used by various high-layer applications. For some common port numbers, you can use

the mnemonic symbols as shortcut. For example, “bgp” can represent the TCP number 179 used by BGP.

III. Defining the Layer-2 ACL

The rules of Layer-2 ACL are defined on the basis of the Layer-2 information such as source MAC address, source VLAN ID, Layer-2 protocol type, Layer-2 ports receiving and forwarding the packet and destination MAC address to process the data packets.

You can use the following command to define the numbered Layer-2 ACL.

Perform the following configuration in corresponding view.

Table 1-6 Defining the Layer-2 ACL

Operation	Command
Enter Layer-2 ACL view(from system view)	**acl** { **number** *acl-number* | **name** *acl-name* **link** } [**match-order** { **config** | **auto** }]
Add a sub-item to the ACL(from Layer-2 ACL view)	**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*]
Delete a sub-item from the ACL(from Layer-2 ACL view)	**undo rule** *rule-id*
Delete one ACL or all the ACL(from system view)	**undo acl** { **number** *acl-number* **| name** *acl-name* | **all** }

Layer-2 ACL can be identified with numbers ranging from 4000 to 4999.

The **interface** in the above command specifies the Layer-2 interface, such as the Ethernet port of a switch.

IV. Defining the user-defined ACL

The user-defined ACL matches any bytes in the first 80 bytes of the Layer-2 data frame with the character string defined by the user and then processes them accordingly. To correctly use the user-defined ACL, you are required to understand the Layer-2 data frame structure. The figure below shows the first 64 bytes of the Layer-2 data frame of SNAP+tag format with the 802.3 standard. (Every letter represents a hexadecimal number and every two letters are one byte.)

```
AA AA AA AA AA AA BB BB BB BB BB BB CC CC DD DD
DD DD EE FF GG HH HH HH II II JJ KK LL LL MM MM
NN NN OO PP QQ QQ RR RR RR RR SS SS SS SS TT TT
UU UU VV VV VV VV WW WW WW WW XY ZZ aa aa bb bb
```

Figure 1-1 The first 64 bytes of data frame

The table below lists the meaning and offset of each letter.

Table 1-7 Letters and their meanings

Letter	Meaning	Offset	Letter	Meaning	Offset
A	Destination MAC address	0	O	TTL field	34
B	Source MAC address	6	P	Protocol number (6 is TCP and 17 is UDP).	35
C	Data frame length field	12	Q	IP checksum	36
D	VLAN tag field	14	R	Source IP address	38
E	DSAP (Destination Service Access Point) field	18	S	Destination IP address	42
F	SSAP (Source Service Access Point) field	19	T	TCP source port	46
G	Ctrl field	20	U	TCP destination port	48
H	org code field	21	V	Sequence number	50
I	Encapsulated Data type	24	W	Acknowledgement field	54
J	IP version	26	XY	IP header length and currently unused bit	58
K	TOS field	27	Z	Currently unused bits and flags bit	59
L	IP packet length	28	a	Window Size field	60
M	ID number	30	b	Others	62
N	Flags field	32			

The offsets listed in the above table are the field offsets in the SNAP+tag 802.3 data frame. In the user-defined ACL, you can use the rule mask and offset parameters to select any bytes from the first 64 bytes of the data frame and compare them with the user-defined rule to filter the matched data frames and process accordingly. The rules defined by the user can be some fixed properties of the data. For example, to filter all the TCP packets, you can define the rule as “06”, the rule mask as “FF” and the offset as 35. In this case, the rule mask coordinates with the offset and picks up the TCP protocol number field from the data frame and compares it with the user-defined rule string to get all the TCP packets.

Note:

When user defines user-defined ACL, please calculate and set the correct offsets according to the data frames of SNAP+tag format with the 802.3 standard described above.

You can use the following commands to define user-defined ACL.

Perform the following configuration in corresponding view.

Table 1-8 Defining the user-defined ACL

Operation	Command
Enter user-defined ACL view(from system view)	**acl** { **number** *acl-number* | **name** *acl-name* **user** } [**match-order** { **config** | **auto }**]
Add a sub-item to the ACL(from user-defined ACL view)	**rule** [*rule-id*] { **permit** | **deny** } { *rule-string rule-mask offset* }&<1-8> [**time-range** *name*]
Delete a sub-item from the ACL(from user-defined ACL view)	**undo rule** *rule-id*
Delete one ACL or all the ACL(from system view)	**undo acl** { **number** *acl-number* | **name** *acl-name* | **all** }

The self-defined ACL are identified with the numbers ranging from 5000 to 5999.

1.2.3 Activating ACL

The defined ACL can be active after activated globally on the switch. This function is used to activate the ACL filtering or classify the data transmitted by the hardware of switch.

You can use the following command to activate the defined ACL.

Perform the following configuration in system view.

Table 1-9 Activating ACL

Operation	Command
Activate an ACL	**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*] }* }
Deactivate an ACL	**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*] }* }

Note:

This command supports the process to activate the Layer-2 and IP ACLs at the same time(IP ACLs include basic and advanced ACLs), however the actions of the combination items should be consistent. If the actions conflict (one is permit and the other is deny), they cannot be activated.

1.2.4 Displaying and Debugging ACL

After the above configuration, execute **display** command in all views to display the running of the ACL configuration, and to verify the effect of the configuration. Execute **reset** command in user view to clear the statistics of the ACL module.

Table 1-10 Displaying and debugging ACL

Operation	Command
Display the status of the time range	**display time-range** { **all** | *name* }
Display the detail information about the ACL	**display acl config** { **all** | *acl-number* | *acl-name* }
Display the information about the ACL running state	**display acl running-packet-filter all**
Clear ACL counters	**reset acl counter** { **all** | *acl-number* | *acl-name* }

The matched information of **display acl config** command specifies the rules treated by the switch's CPU. The matched information of the transmitted data by switch can be displayed by **display qos-global traffic-statistic** command.

For syntax description, refer to the Command Manual.

1.3 ACL Configuration Example

1.3.1 Advanced ACL Configuration Example

I. Networking requirements

The interconnection between different departments on a company network is implemented through the 100M ports of the Ethernet Switch. The payment query server of the Financial Dept. is accessed via Ethernet1/1 (at 129.110.1.2). It is required to properly configure the ACL and limit the department other than the Office of President access the payment query server between 8:00 and 18:00. The Office of President (at 129.111.1.2) can access the server without limitation.

II. Networking diagram

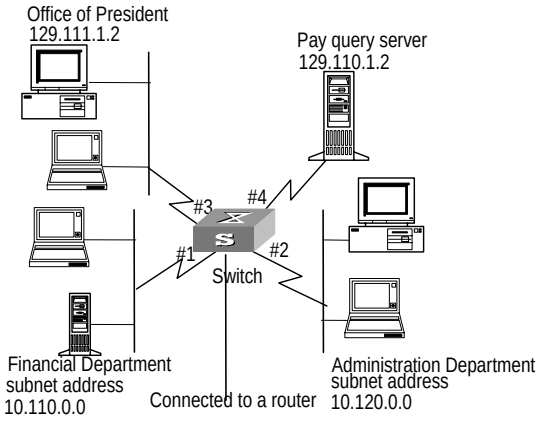


Figure 1-2 Access control configuration example

III. Configuration procedure

Note:

In the following configurations, only the commands related to ACL configurations are listed.

---

1) Define the work time range

Define time range from 8:00 to 18:00.

```
[Quidway] time-range huawei  8:00 to 18:00 working-day
```

2) Define the ACL to access the payment server.

Enter the named advanced ACL, named as traffic-of-payserver.

```
[Quidway] acl name traffic-of-payserver advanced match-order config
```

Define the rules for other department to access the payment server.

```
[Quidway-acl-adv-traffic-of-payserver] rule 1 deny ip source any destination
129.110.1.2 0.0.0.0 time-range huawei
```

Define the rules for the Office of President to access the payment server.

```
[Quidway-acl-adv-traffic-of-payserver] rule 2 permit ip source 129.111.1.2
0.0.0.0 destination 129.110.1.2 0.0.0.0
```

3) Activate ACL.

Activate the ACL traffic-of-payserver .

```
[Quidway] packet-filter ip-group traffic-of-payserver
```

1.3.2 Basic ACL Configuration Example

I. Networking requirements

Using basic ACL, filter the packet which source IP address is 10.1.1.1 during time range 8:00 ~ 18:00 every day.

II. Networking diagram

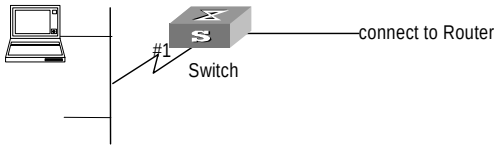


Figure 1-3 Access control configuration example

III. Configuration procedure

Note:

In the following configurations, only the commands related to ACL configurations are listed.

---

1) Define the time range

Define time range from 8:00 to 18:00.

```
[Quidway] time-range huawei 8:00 to 18:00 daily
```

2) Define the ACL for packet which source IP is 10.1.1.1.

Enter the named basic ACL, named as traffic-of-host.

```
[Quidway] acl name traffic-of-host basic
```

Define the rules for packet which source IP is 10.1.1.1.

```
[Quidway-acl-basic-traffic-of-host] rule 1 deny source 10.1.1.1 0 time-range huawei
```

3) Activate ACL.

Activate the ACL traffic-of-host .

```
[Quidway] packet-filter ip-group traffic-of-host
```

1.3.3 Link ACL Configuration Example

I. Networking requirements

Using Link ACL, filter the packet which source MAC address is 00e0-fc01-0101 and destination MAC address is 00e0-fc01-0303 during time range 8:00 ~ 18:00 every day.

II. Networking diagram

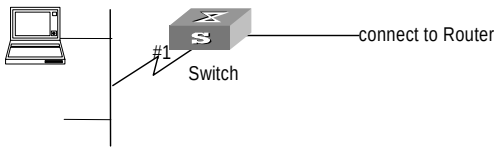


Figure 1-4 Access control configuration example

III. Configuration procedure

Note:

In the following configurations, only the commands related to ACL configurations are listed.

---

1) Define the time range

Define time range from 8:00 to 18:00.

```
[Quidway] time-range huawei 8:00 to 18:00 daily
```

2) Define the ACL for packet which source MAC address is 00e0-fc01-0101 and destination MAC address is 00e0-fc01-0303.

Enter the named link ACL, named as traffic-of-link.

```
[Quidway] acl name traffic-of-link link
```

Define the rules for packet which source MAC address is 00e0-fc01-0101 and destination MAC address is 00e0-fc01-0303.

```
[Quidway-acl-link-traffic-of-link] rule 1 deny ip ingress 00e0-fc01-0101
0-0-0 egress 00e0-fc01-0303 0-0-0 time-range huawei
```

3) Activate ACL.

Activate the ACL traffic-of-link .

```
[Quidway] packet-filter link-group traffic-of-link
```

1.3.4 User-defined ACL Configuration Example

I. Networking requirements

Using user-defined ACL, filter the TCP packet during time range 8:00 ~ 18:00 every day.

II. Networking diagram

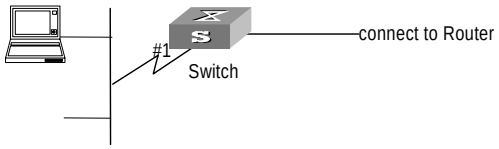


Figure 1-5 Access control configuration example

III. Configuration procedure

Note:

In the following configurations, only the commands related to ACL configurations are listed.

---

1) Define the time range

Define time range from 8:00 to 18:00.

```
[Quidway] time-range huawei 8:00 to 18:00 daily
```

2) Define the ACL for TCP packet.

Enter the named user-defined ACL, named as traffic-of-tcp.

```
[Quidway] acl name traffic-of-tcp user
```

Define the rules for TCP packet.

```
[Quidway-acl-user-traffic-of-tcp] rule 1 deny 06 ff 35 time-range huawei
```

3) Activate ACL.

Activate the ACL traffic-of-tcp .

```
[Quidway] packet-filter user-group traffic-of-tcp
```

Chapter 2 QoS Configuration

2.1 QoS Overview

In the traditional IP network, all the packets are treated equally without priority difference. Every switch/router handles the packets following the First In First Out (FIFO) policy. That is, they make best effort to transmit the packets to the destination, not making any commitment or guarantee of the transmission reliability, delay or to satisfy other performance requirements.

With the rapid development of computer network, people transfer more and more voice, image and important data etc at real time which are sensitive to the bandwidth, delay and jitter. This enriches the network sources. On the other hand, the network congestion occurs more frequently, hence people require higher Quality of Service (QoS) for the transmission over the network.

The Ethernet technology is the most widely used network technology nowadays. Ethernet has been the dominant technology of various independent Local Area Networks (LANs), and many LANs in the Ethernet form have been part of the Internet. Moreover, along with the continuous development of the Ethernet technology, Ethernet will become one of the major ways to access the common Internet users. In order to implement the end-to-end QoS solution on the whole network, it is inevitable to consider the question of how to guarantee the Ethernet QoS service. This requires the Ethernet switching devices to apply the Ethernet QoS technology and deliver the QoS guarantee at different levels to different types of signal transmissions over the networks, especially those having requirements of shorter time delay and lower jitters.

2.1.1 Traffic

Traffic refers to all packets passing through a switch.

2.1.2 Traffic Classification

Traffic classification means identifying the packets with certain characteristics, using the matching rule called classification rule, set by the configuration administrator based on the actual requirements. The rule can be very simple. For example, the traffic with different priorities can be identified according to the ToS field in IP packet header. There are also some complex rules. For example, the information over the integrated link layer (Layer-2), network layer (Layer-3) and transport layer (Layer-4), such as MAC address, IP protocol, source IP address, destination IP address and the port number of application etc can be used for traffic classification. Generally the classification standards are encapsulated in the header of the packets. The packet content is seldom used as the classification standard.

2.1.3 Packet Filter

Packet filter is to filter traffic. For example, the operation “deny” discards the traffic that is matched with a traffic classification rule, while allowing other traffic to pass through. With the complex traffic classification rules, Ethernet Switches enable the filtering of various information carried in Layer 2 traffic to discards the useless, unreliable or doubtful traffic, thereby enhancing the network security.

The two key steps of realizing the frame filtering are as follows.

Step 1: Classify the ingress traffic according to the classification rule;

Step 2: Filter the classified traffic, i.e. the “**deny**” operation, the default ACL operation.

2.1.4 Traffic Policing

In order to deliver better service with the limited network resources, QoS monitors the traffic of the specific user on the ingress, so that it can make a better use of the assigned resource.

2.1.5 Port traffic Limit

The port traffic limit is the port-based traffic limit used for limiting the general speed of packet output on the port.

2.1.6 Redirection

You can specify a new port to forward the packets according to your requirements on the QoS policy.

2.1.7 Traffic Priority

The Ethernet Switch can deliver priority tag service for some special packets. The tags include TOS, DSCP and 802.1p, etc., which can be used and defined in different QoS modules.

2.1.8 Queue Scheduling

When congestion occurs, several packets will compete for the resources. Three kinds of queue scheduling algorithms are used to overcome the problem. These three kinds of queue scheduling algorithms are Strict-Priority Queue (SP), Weighted Round Robin (WRR) and Delay bounded WRR.

1) SP

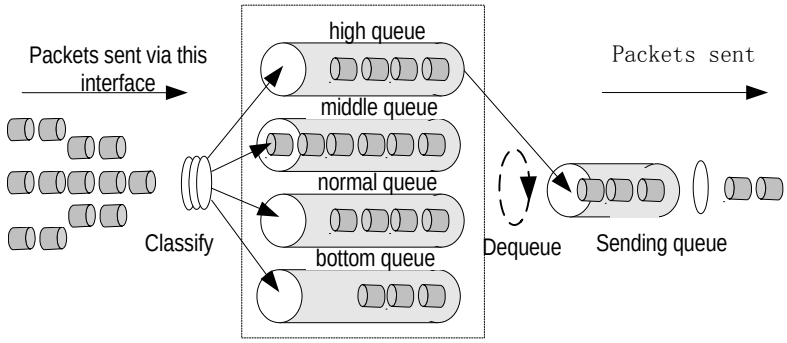


Figure 2-1 SP

The SP is specially designed for the key service application. A significant feature of the key service is requiring for priority to enjoy the service to reduce the responding delay when congestion occurs. Take 4 egress queues for each port as example, SP divides the queue of port into up to 4 kinds, high-priority, medium-priority, normal-priority and low-priority queues (which are shown as the Queue 3, 2, 1 and 0 in turn) with sequentially reduced priority.

During the progress of queue dispatching, strictly following the priority order from high to low, the SP gives preference to and sends the packets in the higher-priority queue first. When the higher-priority queue is empty it will send the packets in the lower-priority group. In this way, put the packets of higher priority service in the higher-priority queue and put the packets of lower priority, like e-mail, in the lower-priority queue, can guarantee the key service packets of higher priority are transmitted first, while the packets of lower service priority are transmitted during the idling gap between transmitting the packets of higher service priorities.

The SP also has the drawback that when congestion occurs, if there are many packets queuing in the higher-priority queue, it will require a long time to transmit these packets of higher service priority while the messages in the lower-priority queue are continuously set aside without service.

2) WRR

The round scheduling ensures every queue gets some time of service of the switch port. Take 4 egress queues for each port as example, WRR gives every queue a weight (w3, w2, w1, and w0 respectively) for resource obtaining. For example, you can configure the weight value of the WRR algorithm for 100M port as 50, 30, 10, 10 (corresponding to the w3, w2, w1 and w0 respectively). Thus the low-priority queue can be guaranteed to get the minimum bandwidth of 10Mbps, avoiding the case in SP scheduling that the messages in the lower-priority queues may not get any service for long time. Another advantage of WRR queue is that the service time is assigned to each queue flexibly, although it is the round multiple queue scheduling. When a queue is empty, it will switch to the next queue immediately, thereby making good used of the bandwidth resource.

3) Delay bounded WRR

Comparing to the common WRR, the Delay bounded WRR also guarantee the packets in the highest-priority queue to leave the queue before the configured delay.

2.1.9 Traffic Mirroring

The traffic mirroring function is carried out by copying the specified data packets to the monitoring port for network diagnosis and troubleshooting.

2.1.10 Traffic Counting

With the flow-based traffic counting, you can request a traffic count to count and analyze the packets.

2.2 Configuring QoS

QoS configuration includes:

- Setting port priority
- Configuring trust packet priority
- Packet filter
- Traffic policing
- Redirection configuration
- Priority tag
- Queue scheduling
- Traffic mirroring
- Traffic statistics

Before configure the about QoS tasks, you have to define the corresponding ACL. Packet filter function can be realized by activate the ACL.

2.2.1 Setting Port Priority

You can use the following command to set the port priority. The switch will tag the packet using the VLAN the received port belong to if the packet has no VLAN tag. Meanwhile the system uses the port priority as the packet the 802.1p priority when tag the packet. If the packet has VLAN tag, the system will not re-tag the packet.

Perform the following configuration in Ethernet port view.

Table 2-1 Setting port priority

Operation	Command
Set the port priority	**priority** *priority-level*
Restore the default port priority	**undo priority**

The port of Ethernet Switch supports 8 priority levels. You can configure the port priority at your requirements.

priority-level ranges from 0 to 7.

By default, the port priority is 0 and switch replaces the priority carried by a packet with the port priority.

2.2.2 Configuring Trust Packet Priority

The switch will tag the packet using the VLAN the received port belong to if the packet has no VLAN tag. Meanwhile the system uses the port priority as the packet the 802.1p priority when tag the packet. If the packet has VLAN tag, the system will not re-tag the packet. User can configure system trusting the packet 802.1p priority and not replacing the 802.1p priorities carried by the packets with the port priority.

Perform the following configuration in Ethernet port view.

Table 2-2 Configuring port priority replacement

Operation	Command
Configure trust packet 802.1p priority	**priority trust**
Configure not trust packet 802.1p priority	**undo priority**

2.2.3 Traffic Policing

Traffic policing is the flow-based traffic limit. It takes corresponding actions to deal with the flow at exceeding speed, such as discarding or lowering the priority.

You can use the following command to configure the traffic policing.

Perform the following configuration in Ethernet port view.

Table 2-3 Configuring traffic limit

Operation	Command
Configure the flow-based traffic limit	**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*]
Cancel the configuration of the flow-based traffic limit	**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*] }* }

You have to define the corresponding ACL before performing this configuration task.

The purpose of this configuration task is to implement the traffic policing over the data flow matching the ACL. The traffic beyond the limit will be dealt with in some other way, such as discarding.

For details about the command, refer to the Command Manual.

2.2.4 Port Traffic Limit

The port traffic limit is the port-based line rate used for limiting the general speed of packet output on the port.

You can use the following command to configure port traffic limit.

Perform the following configuration in Ethernet port view.

Table 2-4 Configuring port traffic limit

Operation	Command
Configure the port traffic limit	**line-rate** *target-rate*
Cancel the configuration port traffic limit	**undo line-rate**

Ethernet Switch supports the function of configuring configure a traffic limit for a single port.

For details about the command, refer to the *Command Manual*.

2.2.5 Configuring Packet Redirection

Packet redirection is to redirect the packets to be forwarded to CPU or other output port.

You can use the following command to configure the packet redirection.

Perform the following configuration in system view.

Table 2-5 Configuring redirection

Operation	Command
Configure redirection	**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* } }
Cancel the redirection configuration	**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*] }* }

Note that the packets redirected to the CPU will not be dealt.

Note:

The configuration of redirection only takes effects on the rules with action **permit**.

For details about the command, refer to the *Command Manual*.

2.2.6 Configuring Priority Marking

The priority marking configuration is a policy to tag the priority for the packets matching the ACL. The new priority can be filled in the priority field of the packet header.

You can use the following command to configure the priority marking.

Perform the following configuration in system view.

Table 2-6 Tag packet priority

Operation	Command
Mark the packet priority	**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* }*
Cancel the packet priority marking	**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*] }* }

Ethernet Switch support a function to tag the packets with IP precedence (specified by **ip-precedence** in the **traffic-priority** command), DSCP (specified by **dscp** in the **traffic-priority** command) or 802.1p preference (specified by cos in the **traffic-priority** command). You can tag the packets with different priorities at requirements on QoS policy. The switch puts the packets into corresponding egress queues according to the 802.1p preference or the local preference (specified by **local-precedence** in the **traffic-priority** command). If both the 802.1p preference and local preference have been specified in the **traffic-priority** command, the switch will put the packets into corresponding queues according to the 802.1p preference first.

For details about the command, refer to the *Command Manual*.

2.2.7 Configuring Queue Scheduling

Queue scheduling is commonly used to resolve the problem that multiple messages compete for resource when the network congestion happens. The queue scheduling function put the packet to output queue of the port according to 802.1p priority of the packet. The mapping relationship between 802.1p priority and output queue of the port is as followed table.

Table 2-7 Default "CoS → Local-precedence" mapping table

CoS Value	Local Precedence
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

Table 2-8 Relationship between 802.1p priority and output queue

802.1p priority	Queue ID
1,2	0
0,3	1
4,5	2
6,7	3

Table 2-9 Relationship between local-precedence and output queue

Local-precedence	Queue ID
0,1	0
2,3	1
4,5	2
6,7	3

I. Configuring the mapping relationship between COS and local precedence

By default, the system provides the default "COS ->Local-precedence" mapping relationship.

Table 2-10 Default "CoS → Local-precedence" mapping table

CoS Value	Local Precedence
0	2
1	0

CoS Value	Local Precedence
2	1
3	3
4	4
5	5
6	6
7	7

Using the following commands, you can configure the maps.

Perform the following configuration in system view.

Table 2-11 Map configuration

Operation	Command
Configure "COS ->Local-precedence" map	**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*
Restore its default value	**undo qos cos-local-precedence-map**

By default, the switch uses the default mapping relationship.

II. Configuring the queue scheduler

You can use the following command to configure the queue scheduler.

Perform the following configuration in system view.

Table 2-12 Configuring the queue scheduling algorithm

Operation	Command
Configure the queue scheduling algorithm	**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* }
Restore the default queue scheduling algorithm	**undo queue-scheduler**

Ethernet Switch support 3 kinds of queue schedulers, i.e., strict-priority, WRR and Delay bounded WRR.

By default, the switch uses the strict-priority algorithm.

For details about the command, refer to the *Command Manual*.

2.2.8 Configuring Traffic Mirroring

The function of Traffic mirroring is to copy the traffic matching ACL rule to the designated observing port to analyze and monitor the packets.

You can use the following command to configure the traffic mirroring.

Perform the following configuration in system view.

Table 2-13 Configuring traffic mirroring

Operation	Command
Configure traffic mirroring	**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*] }* } **interface** { *interface-name* | *interface-type interface-num* }
Cancel the configuration of traffic mirroring	**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*] }* }

For details about the command, refer to the *Command Manual*.

2.2.9 Configuring Traffic Statistics

The traffic statistics function is used for counting the data packets of the specified traffic, that is, this function counts the transmitted data which matches the ACL rules. After the traffic statistics function is configured, the user can use **display qos-global traffic-statistic** command to display the statistics information.

You can use the following command to configure traffic statistics.

Perform the following configuration in system view.

Table 2-14 Configuring traffic statistics

Operation	Command
Configure traffic statistics	**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*] }* }
Cancel the configuration of traffic statistics	**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*] }* }
Display the statistics information	**display qos-global traffic-statistic**

For details about the command, refer to the *Command Manual*.

2.2.10 Displaying and Debugging QoS

After the above configuration, execute display command in all views to display the running of the QoS configuration, and to verify the effect of the configuration. Execute **reset** command in user view to clear the statistics of QoS module.

Table 2-15 Displaying and debugging QoS

Operation	Command
Display the parameter settings of all the QoS actions	**display qos-global all**
Display the mapping relationship between cos and local precedence	**display qos cos-local-precedence-map**
Display the parameter settings of traffic mirroring	**display qos-global mirrored-to**
Display the parameter settings of port mirroring	**display mirror**
Display the queue scheduling mode and parameter	**display queue-scheduler**
Display the settings of QoS	**display qos-interface** [*interface-name* | *interface-type interface-num*] **all**
Display the parameter settings of traffic limit	**display qos-interface** [*interface-name* | *interface-type interface-num*] **traffic-limit**
Display the port traffic limit	**display qos-interface** [*interface-name* | *interface-type interface-num*] **line-rate**
Display the settings of priority tag	**display qos-global traffic-priority**
Display the settings of redirection	**display qos-global traffic-redirect**
Display the information about the traffic	**display qos-global traffic-statistic**
Clear the statistics information	**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*] }* }

For output and description of the related commands, refer to the Command Manual.

2.2.11 QoS Configuration Example

I. Networking requirements

The interconnection between different departments on a company network is implemented through the 100M ports of the Ethernet Switch. The payment query server of the Financial Dept. is accessed via Ethernet0/1 (at 129.110.1.2). It is required to limit the traffic from the server to other department to no more than 20M, set the DSCP

preferences of those not match the rules to 4. And It is required to limit the traffic from other department to the server to no more than 20M.

II. Networking diagram

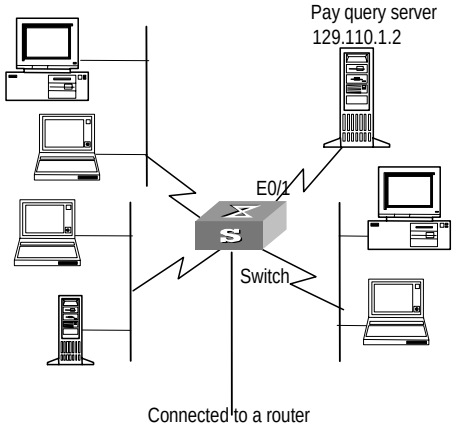


Figure 2-2 Access control configuration example

III. Configuration procedure

Note:

In the following configurations, only the commands related to QoS/ACL configurations are listed.

---

1) Define the traffic accessing the payment query server

Enter the named advanced ACL view, identified as traffic-of-payserver.

```
[Quidway] acl name traffic-of-payserver advanced match-order config
```

Define advanced ACL traffic-of-payserver.

```
[Quidway-acl-adv-traffic-of-payserver] rule 1 permit ip source 129.110.1.2
0.0.0.0 destination any
```

2) Define the limit to the traffic-of-payserver

Limit the average speed of the traffic-of-payserver to 20M, sets the IP precedence of the packets exceeding committed average rate in the traffic to 4.

```
[Quidway-Ethernet0/1] traffic-limit inbound ip-group traffic-of-payserver 20
exceed remark-dscp 4
```

Limit the sending rate of Ethernet0/1 as 20M.

```
[Quidway-Ethernet0/1] line-rate 20
```

Chapter 3 Logon User ACL Control Configuration

3.1 Overview

As the Ethernet switches launched by Huawei Technologies are used more and more widely over the networks, the security issue becomes even more important. The switches provide several logon and device accessing measures, mainly including TELNET access, SNMP access, and HTTP access. The security control over the access measures is provided with the switches to prevent illegal users from logging on to and accessing the devices. There are two levels of security controls. At the first level, the user connection is controlled with ACL filter and only the legal users can be connected to the switch. At the second level, a connected user can log on to the device only if he can pass the password authentication.

This chapter mainly introduces how to configure the first level security control over these access measures, that is, how to configure to filter the logon users with ACL. For detailed description about how to configure the first level security, refer to “getting started” module of Operation Manual.

3.2 Configuring ACL Control over the TELNET Users

Configuring ACL control over the TELNET users can help filter the malicious and illegal connection requests before the password authentication and ensure the device security.

Take the following steps to configure the ACL control over the TELNET users:

1) Defining ACL
2) Calling ACL to control TELNET users

The follow section introduces the configuration procedures.

3.2.1 Defining ACL

You can only call the numbered ACL, ranging from 2000 to 3999, to implement ACL control function.

You can use the following command to configure the basic ACL.

Perform the following configuration in system view.

Table 3-1 Defining the basic ACL

Operation	Command
Enter basic ACL view(from system view)	**acl** { **number** *acl-number* | **name** *acl-name* **basic** } [**match-order** { **config** | **auto** }]
add a sub-item to the ACL(from basic ACL view)	**rule** [*rule-id*] { **permit** | **deny** } [**source** *source-addr wildcard* | **any**] [**fragment**] [**time-range** *name*]
delete a sub-item from the ACL(from basic ACL view)	**undo rule** *rule-id* [**source**] [**fragment**] [**time-range**]
Delete one ACL or all the ACL(from system view)	**undo acl** { **number** *acl-number* | **name** *acl-name* | **all** }

In the defining process, you can configure several rules for an ACL, using the **rule** command repeatedly.

3.2.2 Calling ACL to Control TELNET Users

To control TELNET users with ACL, you can call the defined ACL in user-interface view.

You can use the following command to call an ACL.

Perform the following configuration in corresponding view.

Table 3-2 Calling ACL to control TELNET users

Operation	Command
Enter user-interface view(from system view)	**user-interface** [*type*] *first-number* [*last-number*]
Call an ACL(from user-interface view)	**acl** *acl-number* { **inbound** | **outbound** }

For detailed description of the command, refer to the *Command Manual*.

Note:

Only the numbered ACL can be called for TELNET user control.

3.2.3 Configuration Example

I. Networking requirements

Only permit TELNET user from 10.110.100.52 and 10.110.100.46 access switch.

II. Networking diagram

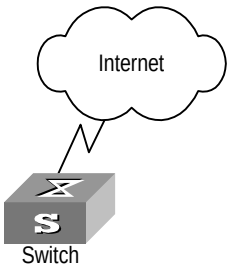


Figure 3-1 Control TELNET users with ACL

III. Configuration procedure

Define the basic ACLs.

```
[Quidway] acl number 2020 match-order config
[Quidway-acl-basic-2020] rule 1 permit source 10.110.100.52 0
[Quidway-acl-basic-2020] rule 2 permit source 10.110.100.46 0
[Quidway-acl-basic-2020] quit
```

Call an ACL.

```
[Quidway] user-interface vty 0 4
[Quidway-user-interface-vty0-4] acl 2020 inbound
```

3.3 Configuring ACL Control over the SNMP Users

Huawei Quidway Ethernet switch series support the remote management with the network management software. The network management users can access the switch with SNMP. Controlling such users with ACL can help filter the illegal NM users and prevent them from accessing the local switch.

Take the following steps to control the SNMP users with ACL.

1) Defining ACL
2) Calling ACL to control SNMP users

The follow section introduces the configuration procedures.

3.3.1 Defining ACL

You can only call the numbered basic ACL, ranging from 2000 to 2999, to implement ACL control function. Use the same configuration commands introduced in the last section.

3.3.2 Calling ACL to Control SNMP Users

To control the NM users with ACL, call the defined ACL when configuring SNMP community name, username, and group name.

You can use the following commands to call an ACL.

Perform the following configuration in system view.

Table 3-3 Defining a numbered basic ACL

Operation	Command
Call an ACL when configuring SNMP community name.	**snmp-agent community** { **read** | **write** } *community-name* [[**mib-view** *view-name*] | [**acl** *acl-number*]]*
Call an ACL when configuring SNMP group name.	**snmp-agent group** { **v1** | **v2c** } *group-name* [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-list*] **snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-list*]
Call an ACL when configuring SNMP username.	**snmp-agent usm-user** { **v1** | **v2c** } *user-name group-name* [**acl** *acl-list*] **snmp-agent usm-user v3** *user-name group-name* [**authentication-mode** { **md5** | **sha** } *auth-password*] [**privacy-mode des56** *priv-password*] [**acl** *acl-list*]

SNMP community name attribute is a feature of SNMP V1. Therefore calling an ACL for SNMP community name configuration can filter the access to SNMP V1network management system.

SNMP group name and username attribute is a feature of SNMP V2C and above. Therefore calling an ACL for SNMP community name configuration can filter the access to the network management system of SNMP V2C or higher. If you configure ACL control in both of the commands, the switch will filter the NM users concerning both the features.

Note:

You can call different ACLs for the above mentioned commands.

For more about the commands, refer to the *Command Manual*.

Note:

Only the numbered basic ACL can be called for network management user control.

3.3.3 Configuration Example

I. Networking requirements

Only permit SNMP user from 10.110.100.52 and 10.110.100.46 access switch.

II. Networking diagram

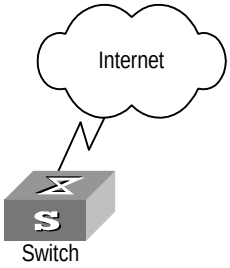


Figure 3-2 Controlling SNMP users with ACL

III. Configuration procedure

Define the basic ACLs.

```
[Quidway] acl number 2020 match-order config
[Quidway-acl-basic-2020] rule 1 permit source 10.110.100.52 0
[Quidway-acl-basic-2020] rule 2 permit source 10.110.100.46 0
[Quidway-acl-basic-2020] quit
```

Call the basic ACLs.

```
[Quidway] snmp-agent community read huawei acl 2020
[Quidway] snmp-agent group v2c huaweigroup acl 2020
[Quidway] snmp-agent usm-user v2c huaweiuser huaweigroup acl 2020
```

3.4 Configuring ACL Control over the HTTP Users

Quidway Ethernet switch series support the remote management through WEB. The users can access the switch through HTTP. Controlling such users with ACL can help filter the illegal users and prevent them from accessing the local switch. After configuring ACL control over these users, the switch allows only one WEB user to access the Ethernet switch at one time.

Take the following steps to control the HTTP users with ACL.

1) Defining ACL
2) Calling ACL to control HTTP users

The follow section introduces the configuration procedures.

3.4.1 Defining ACL

So far, you can only call the numbered basic ACL, ranging from 2000 to 2999, to implement ACL control function. Use the same configuration commands introduced in the last section.

3.4.2 Calling ACL to Control HTTP Users

To control the WEB network management users with ACL, call the defined ACL.

You can use the following commands to call an ACL.

Perform the following configuration in system view.

Table 3-4 Calling ACL to control HTTP users

Operation	Command
Call an ACL to control the WEB NM users.	**ip http acl** *acl-number*
Cancel the ACL control function.	**undo ip http acl**

For more about the commands, refer to the *Command Manual*.

Note:

Only the numbered basic ACL can be called for WEB NM user control.

3.4.3 Configuration Example

I. Networking requirements

Only permit WEB NM user from 10.110.100.46 access switch.

II. Networking diagram

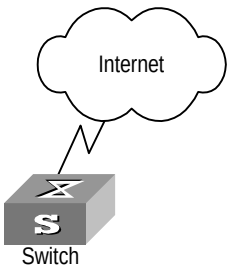


Figure 3-3 Control WEB NM user with ACL

III. Configuration procedure

Define the basic ACL.

```
[Quidway] acl number 2030 match-order config
[Quidway-acl-basic-2030] rule 1 permit source 10.110.100.46 0
[Quidway-acl-basic-2030] quit
```

Call the basic ACL.

```
[Quidway] ip http acl 2030
```

HUAWEI

Quidway S3000-EI Series Ethernet Switches
Operation Manual

Integrated Management

Table of Contents

Chapter 1 Stack Function Configuration

1.1 Stack Function Overview

A stack is a management domain including several Ethernet switches (one main switch and some slave switches) connected through stack ports. These Ethernet switches stacked together can act as one set of equipment and the user can manage them through the main switch.

When several Ethernet switches are connected through stack ports, the user can perform configurations on one switch and set the switch as the main switch in the stack.

A stack is created as follows. First, the user sets the optional IP address pool for the stack, and enables the stack function. Then the system will automatically add the switches, which are connected to the stack ports of the main switch, to the stack. The main switch will distribute usable IP address to the slave switch automatically as the switch joins the stack. If a new switch is connected to the main switch via stack port, the system will automatically add the new switch to the stack after the stack is established.

The connection of stack port automatically establishes the stack relationship. If a slave stack port is disconnected, that slave switch will exit the stack automatically.

1.2 Configure Stack Function

The stack function configuration includes:

- Configure IP address pool for the stack
- Enable/Disable a stack
- Switch to a slave switch view to perform the configuration

1.2.1 Configure IP Address Pool for the Stack

Before enabling a stack, the user shall set an optional IP address range for a stack first. Then the main switch will automatically assign the slave switches with an IP address in the range, when the slave switches are added to the stack.

Perform the following configuration in system view.

Table 1-1 Configure IP address pool for the stack

Operation	Command
Configure IP address range for a stack	**stacking ip-pool** *from-ip-address ip-address-number* [*ip-mask*]
Restore to the default IP address range	**undo stacking ip-pool**

Before setting up a stack, the user should configure a public IP address pool for the slave switch of the stack.

Please note that the above configurations can only be performed on the non-stack switches. After a stack is enabled, the user is prevented from modifying the IP address pool.

1.2.2 Enable/Disable a Stack

When the user enables a stack with the following command, the system will automatically add the switches, connected to the main switch via stack ports, to the stack. After a stack has been enabled, if the stack port is disconnected, slave switch will exit the stack automatically.

Perform the following configuration in system view.

Table 1-2 Enable/Disable a stack

Operation	Command
Enable a stack	**stacking enable**
Disable a stack	**undo stacking enable**

Please note that you can only operate on the main switch to disable a stack.

1.2.3 Switch to a Slave Switch view to Perform the Configuration

The following command can be used to switch from the main switch view to a slave switch view to change the configuration.

Please perform the following configurations in user view.

Table 1-3 Switch to a slave switch view to perform the configuration

Operation	Command
Switch to a slave switch view to perform the configuration	**stacking** *num*

Please note that the above command can only be used for switching from the main switch view to a slave switch view and the user level remains the same after switching. To switch from a slave switch view back to a main switch view, input **quit**.

1.3 Display and Debug Stack Function

After the above configuration, execute **display** command in any view to display the running of the stack configuration, and to verify the effect of the configuration.

Table 1-4 Display and Debug Stack Function

Operation	Command
Display the stack state information on the main switch	**display stacking** [**members**]
Display the stack state information on a slave switch	**display stacking**

When using this command on the main switch, if the input parameter "**members"** is omitted, you will find the displayed information indicating that the local switch is the main switch and also the number of switches in the stack. Using the command with **members**, you will find the member information of the stack, including stack number of main/slave switches, stack name, stack device name, MAC address and status etc.

When using this command on a slave switch, you will find in the displayed information of the slave switch of the stack, the stack number of the switch and MAC address of the main switch in the stack.

1.4 Stack Function Configuration Example

I. Networking requirements

Switch A, Switch B, and Switch C are stacked together through the stack ports. Switch A is the main switch. Switch B and Switch C are slave switches. The network administrator manages Switch B and Switch C through Switch A.

II. Networking diagram

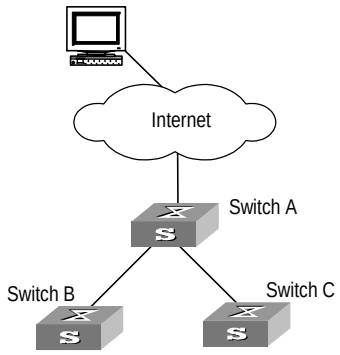


Figure 1-1 Stack configuration example

III. Configuration procedure

Configure IP address pool for the stack on Switch A.

```
[Quidway] stacking ip-pool 129.10.1.1 5
```

Enable a stack on Switch A.

```
[Quidway] stacking enable
```

Display stack information on the main switch, Switch A.

```
<stack_0.Quidway> display stacking
 Main device for stack.
 Total members:3
```

Display stack member information on the main switch, Switch A.

```
<stack_0.Quidway> display stacking members
 Member number: 0
 Name:stack_0.Quidway
 Device: Switch A
 MAC Address:00e0-fc07-0bc0
 Member status:Cmdr

 Member number: 1
 Name:stack_1.Quidway
 Device: Switch B
 MAC Address:00e0-fc07-58a0
 Member status:Up

 Member number: 2
 Name:stack_2.Quidway
 Device: Switch C
 MAC Address:00e0-fc07-58a1
 Member status:Up
```

Switch to the slave switch, Switch B, to perform the configuration.

```
<stack_0.Quidway> stacking 1
<stack_1.Quidway>
```

Display stack information on the slave switch, Switch B.

```
<stack_1.Quidway> display stacking
 Slave device for stack.
 Member number: 1
 Main switch mac address:00e0-fc07-0bc0
```

Switch back to the main switch, Switch A to perform the configuration.

```
<stack_1.Quidway> quit
<stack_0.Quidway>
```

Switch to the slave switch, Switch C, to perform the configuration.

```
<stack_0.Quidway> stacking 2
<stack_2.Quidway>
```

Switch back to the main switch, Switch A to perform the configuration.

```
<stack_2.Quidway> quit
<stack_0.Quidway>
```

Chapter 2 HGMP V2 Configuration

2.1 HGMP V2 Overview

2.1.1 Overview

By HGMP V2 function, the network administrator can manage multiple switches at a managing switch with a public IP address. The managing switch is called *administrator device* and the managed switches are called *member devices*. Generally, you do not assign public IP addresses for the member devices. The management and maintenance over the member devices are implemented through redirection of administrator device. An administrator device and several member devices compose a *cluster*. The figure below illustrates a typical application of the cluster.

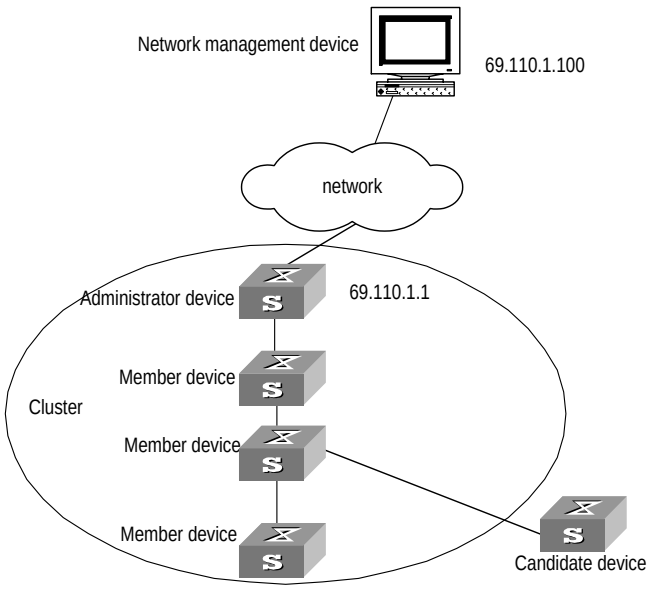


Figure 2-1 A cluster

2.1.2 Role of Switch

The switches in a cluster have different status and functions and play different roles. You can configure the role of a specified switch. And the switches can also change their roles by some defined rules.

The roles in a cluster include administrator device, member device and Candidate device.

- Administrator device: Configured with a public network IP address and providing management interface for all the switches in the cluster. The administrator device manages the member device through command redirection, that is, administrator

device receives and processes the management commands from the network. If the command is destined to a member device, the administrator device will forward it to the member device. The administrator device has the functions such as discovering adjacency information, collecting the topology of the whole network, managing the cluster, maintaining the cluster status and supporting different agents.

- Member device: Member of a cluster, doesn't assigned public IP address, managed by the administrator device's command redirection. The member device has the functions such as discovering adjacent information, being managed by the administrator device, executing the commands delivered by the proxy and reporting failure/log etc.
- Candidate device: Not a member of any cluster yet, but member-capable, that is, being able to be a member device of a cluster.

The following figure illustrates the rules of role switchover.

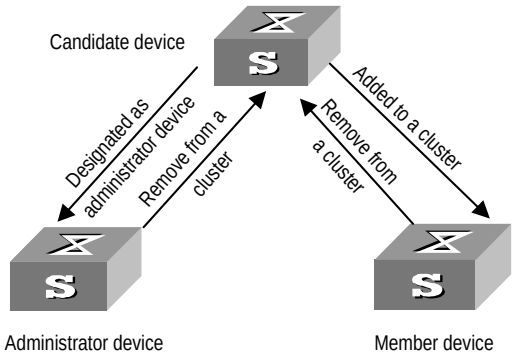


Figure 2-2 Rules of changing roles

- There must be a unique administrator device configured for every cluster. The designated administrator device identifies and discovers the Candidate device through collecting NDP/NTDP information. You can configure a Candidate device as a member device of the cluster.
- After added to a cluster, the Candidate device becomes a member device. If a member device is deleted from the cluster, it becomes a Candidate device again.

Note:

To configure the cluster function, perform the following operations on the administrator device:

- Enable system NDP and port NDP
- Configure NDP parameter
- Enable system NTDP and port NTDP
- Configure NTDP parameter
- Enable cluster function
- Configure cluster parameter

And perform the following operations on the member devices and Candidate devices:

- Enable system NDP and port NDP
- Enable system NTDP and port NTDP
- Enable cluster function

2.1.3 Functions

The advantages of HGMP V2 are as follows:

- Streamlining the configuration management tasks: You can simply configure a public network IP address for the administrator device and thereby implement the configuration and management over multiple switches. There is no need to login to each member device and perform configuration on their Console ports respectively.
- Providing topology discovery and displaying function, which is useful for network displaying and debugging.
- Saving IP address
- Performing software upgrade and parameter configuration to multiple switches simultaneously.
- Independent of network topology and distance.

The HGMP V2 management has the following functions.

- Network topology discovery
- Network topology collection
- Member identification
- Membership management

Detailed functions are described as follows:

- Network topology discovery is implemented by NDP (Neighbor Discovery Protocol). It is used for discovering the information of the directly connected neighbors, including the device type, software/hardware version, connecting port etc. of the adjacent devices and providing the information concerning device ID, port address, device capability and hardware platform etc.

- Network topology collection is implemented by NTDP. It is used for collecting the information concerning device connection and the Candidate device. It can also be used for setting hops for topology discovery.
- Member identification positions every member device in the cluster, so that the administrator device can identify them and delivery the configuration and management commands to them.
- Membership management includes adding or removing a member, member device authenticating the administrator device and hand-shaking interval etc.

The following sections describe the detailed configuration of cluster management functions.

2.2 Configure NDP

2.2.1 NDP Overview

NDP is the protocol for discovering the related information of the adjacent points. NDP runs on the data link layer, so it supports different network layer protocols.

NDP is used for discovering the information of the directly connected neighbors, including the device type, software/hardware version, and connecting port of the adjacent devices. It can also provide the information concerning device ID, port address, device capability and hardware platform, etc.

All the devices supporting NDP maintain the NDP information table. The table entry will be removed by NDP automatically when the aging timer expires. You can also clear the current NDP information to collect new adjacent information.

The device running NDP broadcasts the packets carrying NDP data to all the activated ports regularly. The packet carries the holdtime, indicating how long the receiving device has to keep the updating data. The receiver only keeps the information in the NDP packet, but not forwards it. The corresponding data entry in the NDP table will be updated with the arriving information. If the new information is same as the old one, only the holdtime will be updated.

NDP configuration includes:

- Enable/Disable system NDP
- Enable/Disable port NDP
- Set NDP Holdtime
- Set NDP timer

Note:

On an administrator device, you need to enable system NDP and port NDP, meanwhile configure the NDP parameters as well. However, you only have to enable NDP on a device and the corresponding ports on member device. As the protocol run, the member device will adopt the parameters of the administrator device.

2.2.2 Enable/Disable System NDP

When collecting NDP information of the adjacent device on any port, NDP should be enabled globally. With System NDP, the NDP information will be collected periodically. These information can be queried by user. After disabling System NDP, all the NDP information of the switch will be cleared and the switch will no longer process any NDP packets.

Perform the following configuration in system view.

Table 2-1 Enable/Disable system NDP

Operation	Command
Enable System NDP.	**ndp enable** [**interface** *port-list*]
Disable System NDP.	**undo ndp enable** [**interface** *port-list*]

By default, System NDP is enabled.

2.2.3 Enable/Disable Port NDP

You can set the Port NDP enable/disable states to decide to collect adjacent node information for which port. After system NDP and port NDP have been enabled, the adjacent node NDP information can be collected for the port regularly. If port NDP is disabled, NDP information cannot be collected and transmitted on this port.

Perform the following configuration in Ethernet port view.

Table 2-2 Enable/Disable NDP on a Port

Operation	Command
Enable port NDP	**ndp enable**
Disable port NDP	**undo ndp enable**

By default, port NDP is enabled.

2.2.4 Set NDP Holdtime

The NDP holdtime specifies how long the adjacent node can keep the local node information. The adjacent device knows the holdtime from the received NDP packet and will discard the packet when it expires.

Perform the following configuration in System view.

Table 2-3 Set NDP Holdtime

Operation	Command
Set NDP Holdtime	**ndp timer aging** *aging-in-secs*
Restore the default NDP holdtime.	**undo ndp timer aging**

Note that NDP holdtime is supposed to be longer than the NDP timer (described in the following section). Otherwise, NDP information table will be unstable.

By default, NDP is hold for up to 180 seconds.

2.2.5 Set NDP Timer

The NDP information of the adjacent nodes shall be updated frequently to guarantee the timely updating for local information. You can use the following command to decide how often the NDP information will be updated.

Perform the following configuration in System view.

Table 2-4 Set NDP timer

Operation	Command
Set NDP timer	**ndp timer hello** *seconds*
Set the NDP timer back to the default setting	**undo ndp timer hello**

Note that NDP timer is supposed to be shorter than the NDP holdtime (described in the previous section). Otherwise, NDP information table will be unstable.

By default, NDP is transmitted every 60 seconds.

2.2.6 Display and Debug NDP

After the above configuration, execute **display** command in any view to display the running of the NDP configuration, and to verify the effect of the configuration. Execute **reset** command in user view to clear the statistics of NDP module. Execute **debugging** command in user view to debug the NDP module.

Table 2-5 Display and Debug NDP

Operation	Command
Display global NDP configuration information (including NDP timer and holdtime).	**display ndp**
Display the information about the port enabled with NDP	**display ndp interface** *port-list*
Clear NDP counters.	**reset ndp statistics**
Enable/Disable Debugging NDP	[**undo**] **debugging ndp packet** [**interface** *port-list*]

2.3 Configure NTDP

2.3.1 NTDP Overview

Neighbor Topology Discovery Protocol (NTDP) is a protocol for network topology information collection. NTDP provides the information of available devices to join the cluster and collects the information about switches within the specified hops for the cluster management.

According to the adjacent table information provided by NDP, NTDP transmits and forwards NTDP topology collection request to collect NDP information and neighboring connection information of every device in a certain network. After collecting the information, the administrator device or the network administrator can perform some functions accordingly.

When the NDP on the member device finds changes of neighbor, it will advertise the changes to the administrator device by handshake message. The administrator device can run NTDP to collect the specified topology and show the network topology changes in time.

NTDP configuration includes:

- Enable/Disable Global NTDP
- Enable/Disable NTDP on a Port
- Set hop number for topology collection.
- Set delay for collected device to forward topology collection request
- Set delay for collected port to forward topology collection request
- Set topology collection interval
- Start topology information collection

Note:

On an administrator device, you need to enable system NTDP and port NTDP, meanwhile configure the NTDP parameters as well. However, you only have to enable system NTDP and the corresponding port NTDP on member device. As the protocol run, the member device will adopt the parameters of the administrator device.

2.3.2 Enable/Disable System NTDP

Before a device can process NTDP packet, you are supposed to enable the System NTDP 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.

Perform the following configuration in system view.

Table 2-6 Enable/Disable System NTDP

Operation	Command
Enable System NTDP	**ntdp enable**
Disable System NTDP	**undo ntdp enable**

By default, the System NTDP is enabled.

2.3.3 Enable/Disable Port NTDP

You can use the following command to enable/disable Port NTDP to decide to transmit/receive and forward NTDP packet via which port. After the system 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 packet.

Perform the following configuration in Ethernet port view.

Table 2-7 Enable/Disable port NTDP

Operation	Command
Enable port NTDP	**ntdp enable**
Disable port NTDP	**undo ntdp enable**

Note that, in some occasions, 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.

By default, port NTDP is enabled on the ports supporting NDP. If you enable NTDP on a port not supporting NDP, NTDP cannot be run.

2.3.4 Set Hop Number for Topology Collection

You can set a limit to the hops for topology collection, so that only the topology information of the devices within the specified hops will be collected and infinitive collection can be avoided. The collection scope is limited by setting hop limit for discovery since the switch originating the 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.

Perform the following configuration in system view.

Table 2-8 Set hop number for topology collection.

Operation	Command
Set hop number for topology collection.	**ntdp hop** *hop-value*
Restore the default hop number for topology collection.	**undo ntdp hop**

Note that the settings are only valid on the first switch transmitting the topology collection request. The broader collection scope requires more memory of the topology-collecting device. Normally, collection is launched by the administrator device in cluster function.

By default, the topology information of the switches 3 hops away from the collecting switch is collected.

2.3.5 Set hop-delay and port-delay for Collected Device to Forward Topology Collection Request.

When the topology requests are disseminated over the network, many network devices may receive them at the same time and send responses accordingly, which could cause network congestion and make the topology collector too busy. To avoid such problem, every device delays a duration (hop delay) after receiving a topology request until forwards it via the first port. And then it delays for another duration (port delay) until forwarding it via the next port and so on.

You can use the following commands to configure the hop delay and port delay to forward topology collection request on the current device.

Perform the following configuration in system view.

Table 2-9 Set delay for collected device to forward topology collection request.

Operation	Command
Set delay for collected device to forward topology collection request.	**ntdp timer hop-delay** *time*
Restore the default delay for collected device to forward topology collection request.	**undo ntdp timer hop-delay**
Set delay for collected port to forward topology collection request.	**ntdp timer port-delay** *time*
Restore the default delay for collected port to forward topology collection request.	**undo ntdp timer port-delay**

By default, the device to be collected forwards the topology request after delaying for 200ms, the port to be collected forwards the topology collection request after a delay of 20ms.

2.3.6 Set Topology Collection Interval

In order to learn the global topology changes in time, it is necessary to periodically collect the topology information throughout the whole scope specified.

Perform the following configuration in system view.

Table 2-10 Set topology collection interval

Operation	Command
Set topology collection interval	**ntdp timer** *interval-in-mins*
Restore the default topology collection interval.	**undo ntdp timer**

By default, the value of topology collection is 0, that is, the regular topology collection will not be performed.

2.3.7 Start manually Topology Information Collection

After the topology collection interval is specified, NTDP will automatically and periodically collects topology information throughout the network. Besides, NTDP also provides commands for network topology collection manually.

Whenever you want to manually collect the network topology information for the purpose of device management and monitoring, simply use the following command to start the process.

Perform the following configuration in user view.

Table 2-11 Start topology information collection

Operation	Command
Start topology information collection	**ntdp explore**

2.3.8 Display and Debug NTDP

After the above configuration, execute **display** command in any view to display the running of the NTDP configuration, and to verify the effect of the configuration.

Table 2-12 Display and Debug NTDP

Operation	Command
Display global NTDP information.	**display ntdp**
Display the device information collected by NTDP.	**display ntdp device-list** [**verbose**]

When the **display ntdp device-list** is executed without the **verbose** parameter, it will display the list of the devices collected by NTDP. When executed with the **verbose** parameter, it will display the detailed information about the devices collected by NTDP.

2.4 Configure Cluster

2.4.1 Cluster Overview

This section describes the relevant configurations of cluster management, including how to enable and set up a cluster, how to configure public network IP address for administrator device, how to add/delete a cluster member and how to configure the handshaking interval etc.

There must be a unique administrator device configured for every cluster. A cluster contains only one administrator device. When creating a cluster, you are supposed to designate an administrator device first. It is the entrance and exit to access the cluster members, that is, a user on the external network can access, configure, manage, and monitor the cluster members through it. an administrator device recognizes and controls all the local members, no matter where they are located on the network or how they are connected. In addition, it is responsible for collecting the topology information about all the members and candidates to provide useful information for a user when he establishes a cluster. The administrator device learns the network topology through NDP/NTDP information collection to manage and monitor the device.

Before performing other configuration tasks, the cluster function is supposed to be enabled first.

Cluster configuration includes:

- Enable/Disable cluster function
- Enter cluster view
- Configure cluster IP address pool
- Name the administrator device and cluster.
- Add/delete a cluster member device
- Setup a cluster automatically.
- Member accessing
- Set cluster holdtime.
- Set cluster timer to specify the handshaking message interval.
- Configure FTP/TFTP Servers and Logging/SNMP Hosts for a Cluster.

Note:

You need to enable the cluster function and configure cluster parameters on an administrator device. However, you only have to enable the cluster function on the member devices and Candidate devices.

2.4.2 Enable/Disable Cluster Function

Enable the cluster function before using it.

Perform the following configuration in system view.

Table 2-13 Enable/Disable cluster function

Operation	Command
Enable cluster function.	**cluster enable**
Disable cluster function.	**undo cluster enable**

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.

By default, the cluster function is enabled.

2.4.3 Enter cluster view

You must enter cluster view before configure the cluster function.

Perform the following configuration in system view.

Table 2-14 enter cluster view

Operation	Command
enter cluster view.	**cluster**

2.4.4 Configure Cluster IP Address Pool

Before setting up a cluster, you are supposed to configure a private IP address pool. 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, you can use the administrator device to manage and maintain the member devices.

Perform the following configuration in cluster view.

Table 2-15 Configure cluster IP address pool

Operation	Command
Configure cluster IP address pool.	**ip-pool** *administrator-ip-address { ip-mask | ip-mask-length}*
Restore the default IP address pool of the cluster.	**undo ip-pool**

Before setting up a cluster, the user should configure a private IP address pool for the member devices of the cluster.

Note that, the above configuration can only be performed on administrator device, and must be configured before the cluster is build. The IP address pool of an existing cluster cannot be modified.

2.4.5 Name Administrator device and Cluster

Every cluster has a name.

Perform the following configuration in cluster view.

Table 2-16 Name the administrator device and cluster.

Operation	Command
Name Administrator device and Cluster.	**build** *name*
Remove all the member devices from the cluster and configure the administrator device as a Candidate device.	**undo build**

This command can only be used on an administrator device. When executed on an administrator device to configure a different cluster name, the command can be used to rename the cluster.

By default, the switch is not an administrator device and no cluster name has been specified.

2.4.6 Add/Delete a Cluster Member device

You can use the following command to add a member device or delete a member device.

Perform the following configuration in cluster view.

Table 2-17 Add/Delete a cluster member device

Operation	Command
Add a cluster member device.	**add-member** [*member-num*] **mac-address** *H-H-H* [**password** *password*]
Delete a cluster member device.	**delete-member** *member-num*

Note that, adding/deleting a member device must be performed on the administrator device, otherwise, error prompt will be given.

It is not necessary for you to assign a number for the member device newly added, because the administrator device will assign an available number to it automatically.

When a switch is added to a cluster, the administrator will automatically set administrator's password as the switch's password.

2.4.7 Set up a Cluster Automatically.

The system provides cluster auto-setup function. You can follow the prompts to setup a cluster step by step on an administrator-capable device, using the following command.

After **auto-build** is executed, the system will ask you to enter a cluster name. Then the discovered Candidate devices within the specified hops will be listed. You can confirm the operation and add all the listed candidates to the new cluster.

In the process of automatic setup, you are allowed to enter <CTRL + C> to cancel the operation. And then the system stops adding new switch to the cluster and exits the automatic setup process, however, the switches already added to the cluster will not be removed.

Perform the following configuration in cluster view.

Table 2-18 Automatic cluster setup

Operation	Command
Setup a cluster automatically.	**auto-build** [**recover**]

Note that you can only execute the above command on the command-capable device.

2.4.8 Set Cluster Holdtime

After a cluster is set up, some communication fault maybe occurs due to network problem or switch reset. If the fault has not been addressed before the hold time configured on switch expires, the member state goes down. When the communication is resumed, such member needs to join the cluster again (this process is conducted automatically). Otherwise, the member stays normal and does not to join again.

Perform the following configuration in cluster view.

Table 2-19 Set cluster holdtime

Operation	Command
Set cluster holdtime.	**holdtime** *seconds*
Restore the default cluster holdtime.	**undo holdtime**

Note that the above command can only be executed on the administrator device, which will advertise the cluster timer value to the member devices.

By default, the cluster holdtime is 60 seconds.

2.4.9 Set Cluster Timer to Specify the Handshaking Message Interval

The member devices and administrator device send handshake messages to communicate with each other in real time. The administrator device monitors member states and link states inside the cluster through handshaking with members periodically.

After joining the cluster, a member device starts handshaking with the administrator device regularly. an administrator device and member device consider the current communication as normal, as long as they can receive the handshake messages.

A member or an administrator device considers the communication with each other as failed, if it has not received the handshake messages for three continuous times.

In addition, the member devices send handshake messages to report the topology changes to the administrator device for processing.

You can use the following command to set the handshake message interval on an administrator device.

Perform the following configuration in cluster view.

Table 2-20 Set cluster timer to specify the handshaking message interval.

Operation	Command
Set cluster timer to specify the handshaking message interval.	**timer** *interval*
Restore the default handshaking message interval.	**undo timer**

Note that the above command can only be executed on the administrator device, which will advertise the cluster timer value to the member devices.

By default, handshaking message is transmitted every 10 seconds.

2.4.10 Configure Remote Control over the Member device

The communication between the administrator device and member devices may be interrupted due to some configuration errors. If the member device cannot be controlled in regular way, you can use remote control function provided by administrator device to control member device remotely. For example, you can delete the booting configuration file and reset the member device.

Normally, the cluster packets can only be forwarded over VLAN1. In case of configuration error, for example, the member port connected to the administrator device is configured to VLAN2, the member device and the administrator device will not be able to communicate with each other. However, you can configure VLAN check on the administrator device to solve this problem. After this task is conducted, the configuration information will be contained in the cluster packets. The member device will automatically add the port receiving such packets to VLAN1, if the port does not belong to it. Thus the normal communication between an administrator device and member device is ensured.

You can use the following command to perform the configuration.

Perform the following configuration in cluster view.

Table 2-21 Configure remote control over the member device

Operation	Command
Reset member device	**reboot member** { *member-num* | **mac-address** *H-H-H* } [**eraseflash**]
Configure to perform VLAN check for communication inside the cluster.	**port-tagged vlan** *vlanid*
Configure not to perform VLAN check for communication inside the cluster.	**undo port-tagged**

Note that the above command can only be executed on the administrator device.

When using the **reboot member** command, you can decide to delete the configuration file or not with the **eraseflash** parameter.

2.4.11 Configure the Cluster Server and Network Management and Log Hosts

After a cluster is set up, you can configure the server and network management and log hosts on the administrator device for the entire cluster.

A member device accesses the configured server through the administrator device.

The cluster members output all log information to the configured log host in the end. A member outputs and sends the log information to the administrator device directly. The administrator device translates the log information addresses and sends the log packets to the cluster log host. Similarly, all the trap packets are output to the cluster NM host.

You can use the following commands to configure the cluster server and network management and log hosts.

Perform the following configuration in cluster view.

Table 2-22 Configure FTP /TFTP Servers and Logging/SNMP Hosts for a Cluster

Operation	Command
Configure FTP server for the whole cluster.	**ftp-server** *ip-address*
Remove the FTP server from the cluster.	**undo ftp-server**
Configure TFTP server for the whole cluster.	**tftp-server** *ip-address*
Remove the TFTP server from the cluster.	**undo tftp-server**
Configure the logging host for the whole cluster.	**logging-host** ip-address
Remove the logging host from the whole cluster.	**undo logging-host**
Configure the SNMP host for the whole cluster.	**snmp-host** ip-address
Remove the SNMP host from the whole cluster.	**undo snmp-host**

Note that the above command can only be executed on the administrator device.

2.4.12 Member Accessing

A member device in a cluster can be managed through the administrator device. You can configure a specified member device on administrator device .In order to do this, you should enter the specified member device view on the administrator device; after configuration, you can exit the view.

Authorization is required when you want to configure a switch on the administrator device. Upon passing the member device authorization, the configuration is allowed. If

the user password of the member device is different from the administrator device, you cannot configure the member device. The user level will be inherited from the administrator device when you configure the member device on the administrator device. For example, system will retain in as user view when you configure the member device on the administrator device.

Authorization is also required when you exit the member device view on the administrator device. After passing the authorization, the system will enter user view automatically.

Perform the following configuration in user view.

Table 2-23 Member accessing

Operation	Command
Member accessing	**cluster switch-to** { *member-num* | **mac-address** *H-H-H* | **administrator** }

Note that, when executed on the administrator device, if the parameter *member-num* specifying member number is omitted, error message prompts. Enter **quit** to stop switchover operation.\

2.4.13 Display and Debug Cluster

After the above configuration, execute **display** command in any view to display the running of the Cluster configuration, and to verify the effect of the configuration.

Table 2-24 Display and Debug Cluster

Operation	Command
Display cluster state and statistics	**display cluster**
Display the information of Candidate devices.	**display cluster candidates** [**mac-address** *H-H-H* | **verbose**]
Display the information about member devices.	**display cluster members** [*member-num* | **verbose**]

2.5 HGMP V2 Configuration Example

I. Network requirments

Set up a cluster of three switches and configure an administrator device to manage the other two members. The administrator device is connected with the members via Ethernet0/1 and Ethernet0/2 respectively. It is connected to the external network via

Ethernet1/1 carrying VLAN2 at 163.172.55.1. The entire cluster uses the same FTP server and TFTP server at 63.172.55.1 and the NM station and log host at 69.172.55.4.

II. Networking diagram

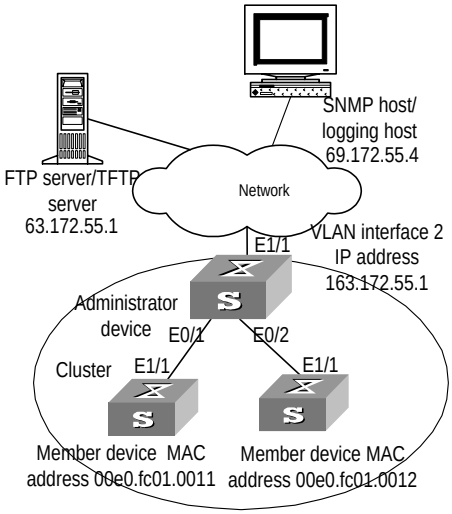


Figure 2-3 HGMP networking

III. Configuration procedure

1) Configure the administrator device

Enable global NDP on the device and port Ethernet0/1 and Ethernet0/2.

```
[Quidway] ndp enable
[Quidway] interface ethernet 0/1
[Quidway-Ethernet0/1] ndp enable
[Quidway-Ethernet0/1] interface ethernet 0/2
[Quidway-Ethernet0/2] ndp enable
```

Set to hold NDP information for 200 seconds.

```
[Quidway] ndp timer aging 200
```

Configure to sends NDP packet every 70 seconds.

```
[Quidway] ndp timer hello 70
```

Enable NTDP on the device and the port Ethernet0/1 and Ethernet0/2.

```
[Quidway] ntdp enable
[Quidway] interface ethernet 0/1
[Quidway-Ethernet0/1] ntdp enable
[Quidway-Ethernet0/1] interface ethernet 0/2
[Quidway-Ethernet0/2] ntdp enable
```

Configure to collect topology information within 2 hops.

```
[Quidway] ntdp hop 2
```

Configure that the collected device delays for 150 milliseconds before forwarding a topology collection request.

```
[Quidway] ntdp timer hop-delay 150
```

Configure that the port on the collected device delays for 15 milliseconds before forwarding a topology collection request.

```
[Quidway] ntdp timer port-delay 15
```

Configure to collect topology information every 3 minutes.

```
[Quidway] ntdp timer 3
```

Run cluster function.

```
[Quidway] cluster enable
```

Configure the internal IP address pool for the cluster, containing 8 addresses starting from 172.16.0.1.

```
[Quidway] cluster
[Quidway-cluster] ip-pool 172.16.0.1 255.255.255.248
```

Set up a cluster and give name to it.

```
[Quidway-cluster] build huawei
[huawei_0.Quidway-cluster]
```

Add the two connected switches into the cluster.

```
[huawei_0.Quidway-cluster] add-member 1 mac-address 00e0-fc01-0011
[huawei_0.Quidway-cluster] add-member 17 mac-address 00e0-fc01-0012
```

Set to hold the member information for 100 seconds.

```
[huawei_0.Quidway-cluster] holdtime 100
[huawei_0.Quidway-cluster] timer 10
```

Configure internal FTP Server, TFTP Server, Logging host, and SNMP host for the cluster.

```
[huawei_0.Quidway-cluster] ftp-server 63.172.55.1
[huawei_0.Quidway-cluster] tftp-server 63.172.55.1
[huawei_0.Quidway-cluster] logging-host 69.172.55.4
[huawei_0.Quidway-cluster] snmp-host 69.172.55.4
```

2) Configure a member device (taking one of the members as an example).

Enable NDP on the device and the port Ethernet1/1.

```
[Quidway] ndp enable
[Quidway] interface ethernet 1/1
[Quidway-Ethernet1/1] ndp enable
```

Enable NTDP on the device and the port Ethernet1/1.

```
[Quidway] ntdp enable
[Quidway] interface ethernet 1/1
```

```
[Quidway-Ethernet1/1] ntdp enable
```

Run the cluster function.

```
[Quidway] cluster enable
```

Note:

Upon the completion of the above configurations, you can use the **cluster switch-to** { *member-num* | **mac-address** *H-H-H* } command to switch to the member device view to maintain and manage the member devices, and use the **cluster switch-to administrator** command to resume the administrator device view. To reset a member device through the administrator device, use the **reboot member** { *member-num* | **mac-address** *H.H.H* } [**eraseflash**] command. For detailed information about these configurations, refer to the preceding description of this chapter.

Chapter 3 Cluster Multicast MAC Address Configuration

3.1 Configuring Cluster Multicast MAC Address

3.1.1 Configuring Cluster Multicast MAC Address

After the establishment of the cluster, you can configure the multicast MAC address which can be learnt by both member and administrative devices for cluster administration. Member devices can learn the multicast information delivered by the administrative device, implementing the delivery of multicast information from the administrative device to the member device. The new multicast MAC address is used when NDP multicast packets, NDTP multicast packet, and HABP multicast packets are sent within the cluster, thus avoiding the transmission problem of BPDU packets of the STP protocol when O/E converter is used.

This configuration procedure only can be used to the administrative device.

Perform the following configuration in cluster view.

Table 3-1 Configure cluster multicast MAC address

Operation	Command
Configure cluster multicast MAC address	**clustetr-mac** *H-H-H*
Configure time interval for sending multicast packets by the administrative device	**cluster-mac syn-interval** *time-interval*

After configuring the cluster multicast MAC address, if the time interval for sending multicast packets by the administrative device is 0, the system prompts you to configure the time interval.

When the time interval is set to 0, the administrative device does not send multicast packets to the cluster member switches.

HUAWEI

Quidway S3000-EI Series Ethernet Switches
Operation Manual

STP

Table of Contents

Chapter 1 MSTP Region-configuration

1.1 MSTP Overview

MSTP stands for Multiple Spanning Tree Protocol, which is compatible with STP and RSTP.

STP cannot transit fast. Even on the point-to-point link or the edge port, it has to take an interval as long as twice forward delay before the network converges.

RSTP can converge fast, but still has the drawback, that is, all the network bridges in a VLAN share a spanning tree and the redundant links cannot be blocked by VLAN.

MSTP makes up for the drawback of STP and RSTP. It makes the network converge fast and the traffic of different VLAN distributed along their respective paths, which provides a better load-balance mechanism for the redundant links.

MSTP associates VLAN and the spanning tree and divides a switching network into several regions, each of which has a spanning tree independent of one another. MSTP prunes the network into a loopfree tree to avoid proliferation, it also provides multiple redundant paths for data forwarding to implement the VLAN data forwarding load-balance.

1.1.1 MSTP Concepts

There are 4 MST region in Figure 1-1. The concept of MSTP will be introduced with this figure in the followed text.

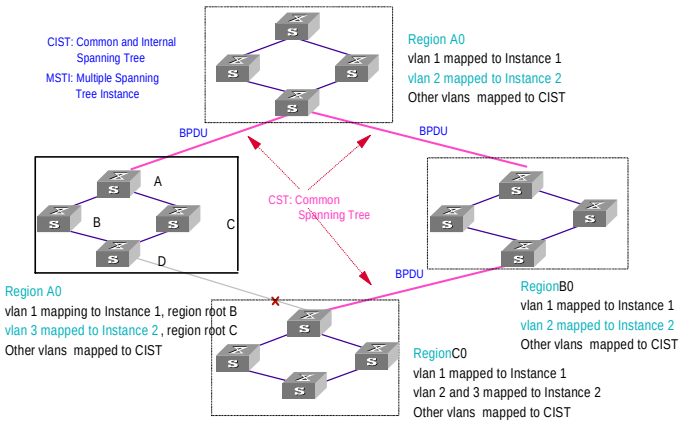


Figure 1-1 Basic MSTP concepts

I. MST region

Multiple Spanning Tree Regions: A multiple spanning tree region contains several physically and directly connected MSTP switches sharing the same region name,

VLAN-spanning tree mapping configuration, and MSTP revision level configuration, and the network segments between them. There can be several MST regions on a switching network. You can group several switches into a MST region, using MSTP configuration commands. For details, refer to the operation manual in this chapter. For example, MST region A0 in the network of figure2-1, the 4 switches in this region are configured same region name, same vlan mapping table (VLAN1 map to instance 1, VLAN 2 map to instance 2, other VLAN map to instance 0), same revision level (not indicated in Figure 1-1).

II. VLAN mapping table

An attribute of MST region, is used for descript the mapping relationship of VLAN and STI. For example, the VLAN mapping table of MST region A0 in figure2-1 is VLAN1 map to instance 1, VLAN 2 map to instance 2, other VLAN map to instance 0.

III. IST

Internal Spanning Tree (IST): The entire switching network has a Common and Internal Spanning Tree (CIST). An MSTP region has an Internal Spanning Tree (IST), which is a fragment of CIST. For example, every MST region in figure2-1 has an IST.

IV. CST

Common Spanning Tree (CST): Connects the spanning trees of all the MST region. Taking every MST region as a “switch”, the CST can be regarded as their spanning tree generated with STP/RSTP. For example, the red line indicates the CST in figure2-1.

V. CIST

CIST (Common and Internal Spanning Tree): A single spanning tree made of IST and CST (Common Spanning Tree). CIST of figure2-1 is composed by each IST in every MST region and the CST.

VI. MSTI

Multiple Spanning Tree Instance (MSTI): Multiple spanning trees can be generated with MSTP in an MSTI and independent of one another. Such a spanning tree is called an MSTI. Every MST region can have many STI called MSTI. These STI is related to corresponding VLAN.

VII. Region root

The region root refers to the root of the IST and MSTI of the MST region. The spanning trees in an MST region have different topology and their region roots may also be different. In each MST region in Figure 1-1, every STI has its region root.

VIII. Common Root Bridge

The Common Root Bridge refers to the root bridge of CIST. There is only one common root bridge in the specified network.

IX. Edge port

The edge port refers to the port located at the MST region edge, connecting different MST regions, MST region and STP region, or MST region and RSTP region. For MSTP calculation, the edge port shall take the same role on MSTI and CIST instance. For example, the edge port as a master port on CIST instance should serve as a master port on every MSTI in the region.

X. Port role

In the process of MSTP calculation, a port can serve as a designated port, root port, master port, Alternate port, or BACKUP.

- The root port is the one through which the data are forwarded to the root.
- The designated port is the one through which the data are forwarded to the downstream network segment or switch.
- Master port is the port connecting the entire region to the Common Root Bridge and located on the shortest path between them.
- Alternate port is the backup of the master port. When the master port is blocked, the alternate port will take its place.
- If two ports of a switch are connected, there must be a loop. In this case, the switch will block one of them. The blocked one is called BACKUP port.

A port can play different roles in different spanning tree instances.

The following figure illustrates the above mentioned concepts for your better understanding.

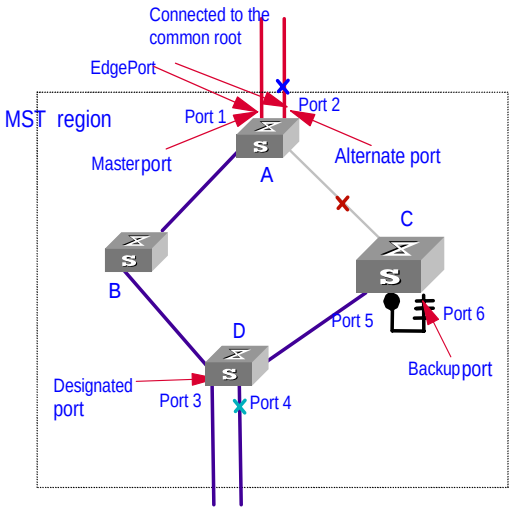


Figure 1-2 Port roles

1.1.2 MSTP Principles

MSTP divides the entire Layer 2 network into several MST regions and calculates and generates CST for them. Multiple spanning trees are generated in a region and each of them is called an MSTI. The instance 0 is called IST, and others are called MSTI.

I. CIST calculation

The CIST root is the highest-priority switch elected from the switches on the entire network through comparing their configuration BPDUs. MSTP calculates and generates IST in an MST region and also the CST connecting the regions. CIST is the unique single spanning tree of the entire switching network.

II. MSTI calculation

Inside an MST region, MSTP generates different MSTIs for different VLANs according to the association between VLAN and the spanning tree. The calculation process of MSTI is same like RSTP.

In this way, the packets of a VLAN travel along the corresponding MSTI inside the MST region and the CST between different regions.

Followed introduce the calculation process of one MSTI.

The fundamental of STP is that the switches exchange a special kind of protocol packet (which is called configuration Bridge Protocol Data Units, or BPDU, in IEEE 802.1D) to decide the topology of the network. The configuration BPDU contains the information enough to ensure the switches to compute the spanning tree.

The configuration BPDU mainly contains the following information:

- The root ID consisting of root priority and MAC address
- The cost of the shortest path to the root
- Designated switch ID consisting of designated switch priority and MAC address
- Designated port ID consisting of port priority and port number
- The age of the configuration BPDU: MessageAge
- The maximum age of the configuration BPDU: MaxAge
- Configuration BPDU interval: HelloTime
- Forward delay of the port: ForwardDelay.

What are the designated switch and designated port?

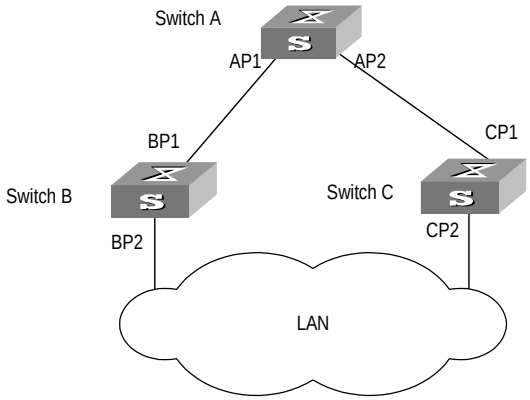


Figure 1-3 Designated switch and designated port

For a switch, the designated switch is a switch in charge of forwarding packets to the local switch via a port called the designated port accordingly. For a LAN, the designated switch is a switch that in charge of forwarding packets to the network segment via a port called the designated port accordingly. As illustrated in the Figure 1-3, Switch A forwards data to Switch B via the port AP1. So to Switch B, the designated switch is Switch A and the designated port is AP1. Also in the figure above, Switch B and Switch C are connected to the LAN and Switch B forwards packets to LAN. So the designated switch of LAN is Switch B and the designated port is BP2.

Note:

AP1, AP2, BP1, BP2, CP1 and CP2 respectively delegate the ports of Switch A, Switch B and Switch C.

- The specific calculation process of STP algorithm.

The following example illustrates the calculation process of STP.

The Figure 1-4 below illustrates the network.

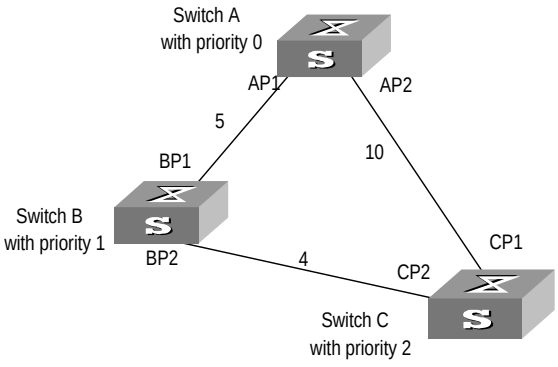


Figure 1-4 Ethernet switch networking

To facilitate the descriptions, only the first four parts of the configuration BPDU are described in the example. They are root ID (expressed as Ethernet switch priority), path cost to the root, designated switch ID (expressed as Ethernet switch priority) and the designated port ID (expressed as the port number). As illustrated in the figure above, the priorities of Switch A, B and C are 0, 1 and 2 and the path costs of their links are 5, 10 and 4 respectively.

1) Initial state

When initialized, each port of the switches will generate the configuration BPDU taking itself as the root with a root path cost as 0, designated switch IDs as their own switch IDs and the designated ports as their ports.

Switch A:

Configuration BPDU of AP1: {0, 0, 0, AP1}

Configuration BPDU of AP2: {0, 0, 0, AP2}

Switch B:

Configuration BPDU of BP1: {1, 0, 1, BP1}

Configuration BPDU of BP2: {1, 0, 1, BP2}

Switch C:

Configuration BPDU of CP2: {2, 0, 2, CP2}

Configuration BPDU of CP1: {2, 0, 2, CP1}

2) Select the optimum configuration BPDU

Every switch transmits its configuration BPDU to others. When a port receives a configuration BPDU with a lower priority than that of its own, it will discard the message and keep the local BPDU unchanged. When a higher-priority configuration BPDU is received, the local BPDU is updated. And the optimum configuration BPDU will be elected through comparing the configuration BPDUs of all the ports.

The comparison rules are:

- The configuration BPDU with a smaller root ID has a higher priority
- If the root IDs are the same, perform the comparison based on root path costs. The cost comparison is as follows: the path cost to the root recorded in the configuration BPDU plus the corresponding path cost of the local port is set as S, the configuration BPDU with a smaller S has a higher priority.
- If the costs of path to the root are also the same, compare in sequence the designated switch ID, designated port ID and the ID of the port via which the configuration BPDU was received.

In summary, we assume that the optimum BPDU can be selected through root ID comparison in the example.

3) Specify the root port, block the redundancy link and update the configuration BPDU of the designated port.

The port receiving the optimum configuration BPDU is designated to be the root port, whose configuration BPDU remains the same. Any other port, whose configuration BPDU has been updated in the step *Select the optimum configuration BPDU*, will be blocked and will not forward any data, in addition, it will only receive but not transmit BPDU and its BPDU remains the same. The port, whose BPDU has not been updated in the step *Select the optimum configuration BPDU* will be the designated port. Its configuration BPDU will be modified as follows: substituting the root ID with the root ID in the configuration BPDU of the root port, the cost of path to root with the value made by the root path cost plus the path cost corresponding to the root port, the designated switch ID with the local switch ID and the designated port ID with the local port ID.

The comparison process of each switch is as follows.

Switch A:

AP1 receives the configuration BPDU from Switch B and finds out that the local configuration BPDU priority is higher than that of the received one, so it discards the received configuration BPDU. The configuration BPDU is processed on the AP2 in a similar way. Thus Switch A finds itself the root and designated switch in the configuration BPDU of every port; it regards itself as the root, retains the configuration BPDU of each port and transmits configuration BPDU to others regularly thereafter. By now, the configuration BPDUs of the two ports are as follows:

Configuration BPDU of AP1: {0, 0, 0, AP1}.

Configuration BPDU of AP2: {0, 0, 0, AP2}.

Switch B:

BP1 receives the configuration BPDU from Switch A and finds that the received BPDU has a higher priority than the local one, so it updates its configuration BPDU.

BP2 receives the configuration BPDU from Switch C and finds that the local BPDU priority is higher than that of the received one, so it discards the received BPDU.

By now the configuration BPDUs of each port are as follows: Configuration BPDU of BP1: {0, 0, 0, AP1}, Configuration BPDU of BP2: {1, 0, 1, BP2}.

Switch B compares the configuration BPDUs of the ports and selects the BP1 BPDU as the optimum one. Thus BP1 is elected as the root port and the configuration BPDUs of Switch B ports are updated as follows.

The configuration BPDU of the root port BP1 retains as {0, 0, 0, BP1}. BP2 updates root ID with that in the optimum configuration BPDU, the path cost to root with 5, sets the designated switch as the local switch ID and the designated port ID as the local port ID. Thus the configuration BPDU becomes {0, 5, 1, BP2}.

Then all the designated ports of Switch B transmit the configuration BPDUs regularly.

Switch C:

CP2 receives from the BP2 of Switch B the configuration BPDU {1, 0, 1, BP2} that has not been updated and then the updating process is launched. {1, 0, 1, BP2}.

CP1 receives the configuration BPDU {0, 0, 0, AP2} from Switch A and Switch C launches the updating. The configuration BPDU is updated as {0, 0, 0, AP2}.

By comparison, CP1 configuration BPDU is elected as the optimum one. The CP1 is thus specified as the root port with no modifications made on its configuration BPDU. However, CP2 will be blocked and its BPDU also remains same, but it will not receive the data (excluding the STP packet) forwarded from Switch B until spanning tree calculation is launched again by some new events. For example, the link from Switch B to C is down or the port receives any better configuration BPDU.

CP2 will receive the updated configuration BPDU, {0, 5, 1, BP2}, from Switch B. Since this configuration BPDU is better then the old one, the old BPDU will be updated to {0, 5, 1, BP2}.

Meanwhile, CP1 receives the configuration BPDU from Switch A but its configuration BPDU will not be updated and retain {0, 0, 0, AP2}.

By comparison, the configuration BPDU of CP2 is elected as the optimum one, CP2 is elected as the root port, whose BPDU will not change, while CP1 will be blocked and retain its BPDU, but it will not receive the data forwarded from Switch A until spanning tree calculation is triggered again by some changes. For example, the link from Switch B to C as down.

Thus the spanning tree is stabilized. The tree with the root Switch A is illustrated in the Figure 1-5 below.

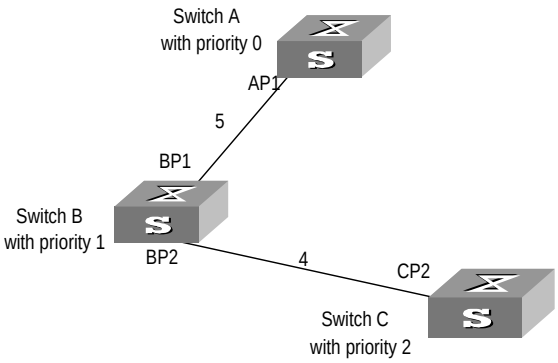


Figure 1-5 The final stabilized spanning tree

To facilitate the descriptions, the description of the example is simplified. For example, the root ID and the designated switch ID in actual calculation should comprise both switch priority and switch MAC address. Designated port ID should comprise port priority and port MAC address. In the updating process of a configuration BPDU, other configuration BPDUs besides the first four items will make modifications according to certain rules. The basic calculation process is described below:

- Configuration BPDU forwarding mechanism in STP:

Upon the initiation of the network, all the switches regard themselves as the roots. The designated ports send the configuration BPDUs of local ports at a regular interval of HelloTime. If it is the root port that receives the configuration BPDU, the switch will enable a timer to time the configuration BPDU as well as increase MessageAge carried in the configuration BPDU by certain rules. If a path goes wrong, the root port on this path will not receive configuration BPDUs any more and the old configuration BPDUs will be discarded due to timeout. Hence, recalculation of the spanning tree will be initiated to generate a new path to replace the failed one and thus restore the network connectivity.

However, the new configuration BPDU as now recalculated will not be propagated throughout the network right away, so the old root ports and designated ports that have not detected the topology change will still forward the data through the old path. If the new root port and designated port begin to forward data immediately after they are elected, an occasional loop may still occur. In RSTP, a transitional state mechanism is thus adopted to ensure the new configuration BPDU has been propagated throughout the network before the root port and designated port begin to send data again. That is, the root port and designated port should undergo a transitional state for a period of Forward Delay before they enter the forwarding state.

MSTP is compatible with STP and RSTP. The MSTP switch can recognize both the STP and RSTP packets and calculate the spanning tree with them. Beside the basic MSTP functions, Quidway Ethernet Switch Series also provide some features easy to manage from the point of view of the users. These features include root bridge hold, secondary root bridge, ROOT PROTECTION, BPDU PROTECTION, protocol hot swapping, master/slave switchover, and so on.

1.2 Configure MSTP

MSTP configuration includes:

- Configure the MST region for a switch
- Specify the switch as primary or secondary root switch
- Configure the MSTP running mode
- Configure the Bridge priority for a switch
- Configure the max hops in an MST region
- Configure the switching network diameter
- Configure the time parameters of a switch
- Configure the max transmission speed on a port
- Configure a port as an edge port
- Configure the Path Cost of a port
- Configure the priority of a port
- Configure the port (not) to connect with the point-to-point link
- Configure the mCheck variable of a port
- Configure the switch security function

- Enable MSTP on the device
- Enable MSTP on a port

Only after MSTP is enabled on the device will other configurations take effect. Before enabling MSTP, you can configure the related parameters of the device and Ethernet ports, which will take effect upon enabling MSTP and stay effective even after resetting MSTP. The **check** command can show the region parameters yet to take effect. The **display active-region-configuration** command shows the parameters configured before MSTP is enabled. For those configured after MSTP is enabled, you can use the related **display** commands to display. For detailed information, refer to the “Display and Debug MSTP” section. .

You do not have to perform all the mentioned tasks to configure MSTP. Many of them are designed to adjust the MSTP parameters provided with default values. You can configure these parameters per the actual conditions or simply take the defaults. For detail information, refer to the task description or the *Command Manual*.

Note:

When GVRP and MSTP startup on the switch simultaneously, GVRP packets will propagate along CIST which is a spanning tree instance. In this case, if you want to issue a certain VLAN through GVRP on the network, you should make sure that the VLAN is mapped to CIST when configuring the VLAN mapping table of MSTP.
CIST is spanning tree instance 0.

1.2.1 Configure the MST Region for a Switch

Which MST region a switch belongs to is determined with the configurations of the region name, VLAN mapping table, and MSTP revision level. You can perform the following configurations to put a switch into an MST region.

Follow the procedure listed in the table below and perform these configurations from system view.

I. Enter MST region view

Perform the following configuration in system view.

Table 1-1 Enter MST region view

Operation	Command
Enter MST region view (from system view)	**stp region-configuration**
Restore the default settings of MST region	**undo stp region-configuration**

II. Configure the MST Region

Perform the following configuration in MST region view.

Table 1-2 Configure the MST region for a switch

Operation	Command
Configure MST region name	**region-name** *name*
Restore the default MST region name	**undo region-name**
Configure VLAN mapping table	**instance** *instance-id* **vlan** *vlan-list*
Restore the default VLAN mapping table	**undo instance**
Configure the MSTP revision level of MST region	**revision-level** *level*
Restore the MSTP revision level of MST region	**undo revision-level**

An MST region can contain up to 17 spanning tree instances, among which the Instance 0 is IST and the Instances 1 through 16 are MSTIs. Upon the completion of the above configurations, the current switch is put into a specified MST region. Note that two switches belong to the same MST region only if they have been configured with the same MST region name, STI-VLAN mapping tables of an MST region, and the MST region revision level.

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 triggers to recalculate the spanning tree according to the configurations only if one of the following conditions is met:

- The user manually activates the configured parameters related to the MST region, using the **active region-configuration** command.
- The user enables MSTP, using the **stp enable** command.

By default, the MST region name is the first switch MAC address, all the VLANs in the MST region are mapped to the STI 0, and the MSTP region revision level is 0. You can restore the default settings of MST region, using the **undo stp region-configuration** command in system view.

III. Activate the MST Region Configuration,and exit the MST Region View

Perform the following configuration in MST region view.

Table 1-3 Activate the MST Region Configuration and exit the MST Region View

Operation	Command
Show the configuration information of the MST region under revision (from MST region view)	**check region-configuration**

Operation	Command
Manually activate the MST region configuration (from MST region view)	**active region-configuration**
Exit MST region view (from MST region view)	**quit**

1.2.2 Specify the Switch as Primary or Secondary Root Switch

MSTP can determine the spanning tree root through calculation. You can also specify the current switch as the root, using the command provided by the switch.

You can use the following commands to specify the current switch as the primary or secondary root of the spanning tree.

Perform the following configuration in system view.

Table 1-4 Specify the switch as primary or secondary root switch

Operation	Command
Specify current switch as the primary root switch of the specified spanning tree.	**stp** [**instance** *instance-id*] **root primary** [**bridge-diameter** *bridgenum*] [**hello-time** *centi-senconds*]
Specify current switch as the secondary root switch of the specified spanning tree.	**stp** [**instance** *instance-id*] **root secondary** [**bridge-diameter** *bridgenum*] [**hello-time** *centi-senconds*]
Specify current switch not to be the primary or secondary root.	**undo stp** [**instance** *instance-id*] **root**

After a switch is configured as primary root switch or secondary root switch, user can't modify the bridge priority of the switch.

You can configure the current switch as the primary or secondary root switch of the STI (specified by the **instance** *instance-id* parameter). If the *instance-id* takes 0, the current switch is specified as the primary or secondary root switch of the CIST.

The root types of a switch in different STIs are independent of one another. The switch can be a primary or secondary root of any STI. However, it cannot serve as both the primary and secondary roots of one STI.

If the primary root is down or powered off, the secondary root will take its place, unless you configure a new primary root. Of two or more configured secondary root switches, MSTP selects the one with the smallest MAC address to take the place of the failed primary root.

When configuring the primary and secondary switches, you can also configure the network diameter and hello time of the specified switching network. For detailed

information, refer to the configuration tasks “Configure switching network diameter” and “Configure the Hello Time of the switch”.

Note:

- You can configure the current switch as the root of several STIs, however, it is not necessary to specify two or more roots for an STI. In other words, please do not specify the root for an STI on two or more switches.
- You can configure more than one secondary root for a spanning tree through specifying the secondary STI root on two or more switches.
- Generally, you are recommended to designate one primary root and more than one secondary roots for a spanning tree.

By default, a switch is neither the primary root or the secondary root of the spanning tree.

1.2.3 Configure the MSTP Running Mode

MSTP and RSTP are compatible and they can recognize the packets of each other. However, STP cannot recognize MSTP packets. To implement the compatibility, MSTP provides two operation modes, STP-compatible mode and MSTP mode. In STP-compatible mode, the switch sends STP packets via every port and serves as a region itself. In MSTP mode, the switch ports send MSTP or STP packets (when connected to the STP switch) and the switch provides multiple spanning tree function.

You can use the following command to configure MSTP running mode. MSTP can intercommunicate with STP. If there is STP switch in the switching network, you may use the command to configure the current MSTP to run in STP-compatible mode, otherwise, configure it to run in MSTP mode.

Perform the following configuration in system view.

Table 1-5 Configure the MSTP running mode

Operation	Command
Configure MSTP to run in STP-compatible mode	**stp mode stp**
Configure MSTP to run in RSTP mode	**stp mode rstp**
Configure MSTP to run in MSTP mode.	**stp mode mstp**
Restore the default MSTP running mode	**undo stp mode**

Generally, if there is STP switch on the switching network, the port connected to it will automatically transit from MSTP mode to STP-compatible mode. But the port cannot automatically transit back to MSTP mode after the STP switch is removed.

By default, MSTP runs in MSTP mode.

1.2.4 Configure the Bridge Priority for a Switch

Whether a switch can be elected as the spanning tree root depends on its Bridge priority. The switch configured with a smaller Bridge priority is more likely to become the root. An MSTP switch may have different priorities in different STIs.

You can use the following command to configure the Bridge priorities of the designated switch in different STIs.

Perform the following configuration in system view.

Table 1-6 Configure the Bridge priority for a switch

Operation	Command
Configure the Bridge priority of the designated switch.	**stp** [**instance** *instance-id*] **bridge-priority** *priority*
Restore the default Bridge priority of the designated switch.	**undo stp** [**instance** *instance-id*] **bridge-priority**

When configuring the switch priority with the **instance** *instance-id* parameter as 0, you are configuring the CIST priority of the switch.

Caution:

In the process of spanning tree root election, of two or more switches with the lowest Bridge priorities, the one has a smaller MAC address will be elected as the root.

By default, the switch Bridge priority is 32768.

1.2.5 Configure the Max Hops in an MST Region

The scale of MST region is limited by the max hops in an MST region, which is configured on the region root. As the BPDU traveling from the spanning tree root, each time when it is forwarded by a switch, the max hops is reduced by 1. The switch discards the configuration BPDU with 0 hops left. This makes it impossible for the switch beyond the max hops to take part in the spanning tree calculation, thereby limiting the scale of the MST region.

You can use the following command to configure the max hops in an MST region.

Perform the following configuration in system view.

Table 1-7 Configure the max hops in an MST region

Operation	Command
Configure the max hops in an MST region.	**stp max-hops** *hop*
Restore the default max hops in an MST region	**undo stp max-hops**

The more the hops in an MST region, the larger the scale of the region. Only the max hops configured on the region root can limit the scale of MST region. Other switches in the MST region also apply the configurations on the region root, even if they have been configured with max hops.

By default, the max hops of an MST is 20.

1.2.6 Configure the Switching Network Diameter

Any two hosts on the switching network are connected with a specific path carried by a series of switches. Among these paths, the one passing more switches than all others is the network diameter, expressed as the number of passed switches.

You can use the following command to configure the diameter of the switching network.

Perform the following configuration in system view.

Table 1-8 Configure the switching network diameter

Operation	Command
Configure the switching network diameter.	**stp bridge-diameter** *bridgenum*
Restore the default switching network diameter.	**undo stp bridge-diameter**

The network diameter is the parameter specifying the network scale. The larger the diameter, the lager the scale.

When a user configures the network diameter on a switch, MSTP automatically calculates and sets the hello time, forward-delay time and maximum-age time of the switch to the desirable values.

Setting the network diameter takes effect on CIST only, but has no effect on MSTI.

By default, the network diameter is 7 and the three corresponding timers take the default values.

1.2.7 Configure the Time Parameters of a Switch

The switch has three time parameters, Forward Delay, Hello Time, and Max Age.

Forward Delay is the switch state transition mechanism. The spanning tree will be recalculated upon link faults and its structure will change accordingly. However, the configuration BPDU recalculated cannot be immediately propagated throughout the network. The temporary loops may occur if the new root port and designated port forward data right after being elected. Therefore the protocol adopts a state transition mechanism. It takes a Forward Delay interval for the root port and designated port to transit from the learning state to forwarding state. The Forward Delay guarantees a period of time during which the new configuration BPDU can be propagated throughout the network.

The switch sends Hello packet periodically at an interval specified by Hello Time to check if there is any link fault.

Max Age specifies when the configuration BPDU will expire. The switch will discard the expired configuration BPDU.

You can use the following command to configure the time parameters for the switch.

Perform the following configuration in system view.

Table 1-9 Configure the time parameters of a switch

Operation	Command
Configure Forward Delay on the switch.	**stp timer forward-delay** *centiseconds*
Restore the default Forward Delay of the switch.	**undo stp timer forward-delay**
Configure Hello Time on the switch.	**stp timer hello** *centiseconds*
Restore the default Hello Time on the switch.	**undo stp timer hello**
Configure Max Age on the switch.	**stp timer max-age** *centiseconds*
Restore the default Max Age on the switch.	**undo stp timer max-age**

Every switch on the switching network adopts the values of the time parameters configured on the root switch of the CIST.

Caution:

- The Forward Delay configured on a switch depends on the switching network diameter. Generally, the Forward Delay is supposed to be longer when the network diameter is longer. Note that too short a Forward Delay may redistribute some redundant routes temporarily, while too long a Forward Delay may prolong the network connection resuming. The default value is recommended.
- A suitable Hello Time ensures the switch to detect the link fault on the network but occupy moderate network resources. The default value is recommended. If you set too long a Hello Time, when there is packet dropped over a link, the switch may consider it as link fault and the network device will recalculate the spanning tree accordingly. However, for too short a Hello Time, the switch frequently sends configuration BPDU, which adds its burden and wastes the network resources.
- Too short a Max Age may cause the network device frequently calculate the spanning tree and mistake the congestion as link fault. However, if the Max Age is too long, the network device may not be able to discover the link fault and recalculate the spanning tree in time, which will weaken the auto-adaptation capacity of the network. The default value is recommended.

To avoid frequent network flapping, the values of Hello Time, Forward Delay and Maximum Age should guarantee the following formulas equal.

2 * (forward-delay - 1seconds) >= maximum-age

maximum-age >= 2 * (hello + 1.0 seconds)

You are recommended to use the **stp root primary** command to specify the network diameter and Hello Time of the switching network, thus MSTP will automatically calculate and give the rather desirable values.

By default, Forward Delay is 15 seconds, Hello Time is 2 seconds, and Max Age is 20 seconds.

1.2.8 Configure the Max Transmission Speed on a Port

The max transmission speed on a port specifies how many MSTP packets will be transmitted every Hello Time via the port.

The max transmission speed on a port is limited by the physical state of the port and the network structure. You can configure it according the network conditions.

You can configure the max transmission speed on a port in the following ways.

I. Configure in system view

Perform the following configuration in system view.

Table 1-10 Configure the max transmission speed on a port

Operation	Command
Configure the max transmission speed on a port.	**stp interface** *interface-list* **transit-limit** *packetnum*
Restore the max transmission speed on a port.	**undo stp interface** *interface-list* **transit-limit**

II. Configure in Ethernet port view

Perform the following configuration in Ethernet port view.

Table 1-11 Configure the max transmission speed on a port

Operation	Command
Configure the max transmission speed on a port.	**stp transit-limit** *packetnum*
Restore the max transmission speed on a port.	**undo stp transit-limit**

You can configure the max transmission speed on a port with either of the above-mentioned measures. For more about the commands, refer to the *Command Manual*.

This parameter only takes a relative value without units. If it is set too large, too many packets will be transmitted during every Hello Time and too many network resourced will be occupied. The default value is recommended.

By default, the max transmission speed on every Ethernet port of the switch is 3.

1.2.9 Configure a Port as an Edge Port

An edge port refers to the port not directly connected to any switch or indirectly connected to a switch over the connected network.

You can configure a port as an edge port or non-edge port in the following ways.

I. Configure in system view

Perform the following configuration in system view.

Table 1-12 Configure a port as an edge port or a non-edge port

Operation	Command
Configure a port as an edge port.	**stp interface** *interface-list* **edged-port enable**
Configure a port as a non-edge port.	**stp interface** *interface-list* **edged-port disable**

Operation	Command
Restore the default setting, non-edge port, of the port.	**undo stp interface** *interface-list* **edged-port**

II. Configure in Ethernet port view

Perform the following configuration in Ethernet port view.

Table 1-13 Configure a port as an edge port or a non-edge port

Operation	Command
Configure a port as an edge port.	**stp edged-port enable**
Configure a port as a non-edge port.	**stp edged-port disable**
Restore the default setting, non-edge port, of the port.	**undo stp edged-port**

You can configure a port as an edge port or a non-edge port with either of the above-mentioned measures. For more about the commands, refer to the *Command Manual*.

After configured as an edge port, the port can fast transit from blocking state to forwarding state without any delay. In the case that BPDU protection has not been enabled on the switch, the configured edge port will turn into non-edge port again when it receives BPDU from other port. In the case that BPDU protection is enabled, the port will be disabled. The configuration of this parameter takes effect on all the STIs. In other words, if a port is configured as an EdgedPort or Non- EdgedPort, it is configured the same on all the STIs.

It is better to configure the BPDU protection on the edged port, so as to prevent the switch from being attacked.

Before BPDU protection is enabled on the switch, the port runs as a non-edge port when it receives BPDU, even if the user has set it as an edge port.

By default, all the Ethernet ports of the switch have been configured as non-edge ports.

Note:

It is better to configure the port directly connected with terminal as the edged port, and enable the BPDU function on the port. That is to realize fast state-transition and prevent the switch from being attacked.

1.2.10 Configure the Path Cost of a Port

Path Cost is related to the speed of the link connected to the port. On the MSTP switch, a port can be configured with different path costs for different STIs. Thus the traffic from different VLANs can run over different physical links, thereby implementing the VLAN-based load-balancing.

You can configure the path cost of a port in the following ways.

I. Configure in system view

Perform the following configuration in system view.

Table 1-14 Configure the Path Cost of a port

Operation	Command
Configure the Path Cost of a port.	**stp interface** *interface-list* [**instance** *instance-id*] **cost** *cost*
Restore the default path cost of a port.	**undo stp interface** *interface-list* [**instance** *instance-id*] **cost**

II. Configure in Ethernet port view

Perform the following configuration in Ethernet port view.

Table 1-15 Configure the Path Cost of a port

Operation	Command
Configure the Path Cost of a port	**stp** [**instance** *instance-id*] **cost** *cost*
Restore the default path cost of a port.	**undo stp** [**instance** *instance-id*] **cost**

You can configure the path cost of a port with either of the above-mentioned measures. For more about the commands, refer to the *Command Manual*.

Upon the change of path cost of a port, MSTP will recalculate the port role and transit the state. When *instance-id* takes 0, it indicates to set the path cost on the CIST.

By default, MSTP is responsible for calculating the port path cost.

1.2.11 Configure the Priority of a Port

For spanning tree calculation, the port priority is an importance factor to determine if a port can be elected as the root port. With other things being equal, the port with the highest priority will be elected as the root port. On the MSTP switch, a port can have different priorities in different STIs and plays different roles respectively. Thus the traffic from different VLANs can run over different physical links, thereby implementing the VLAN-based load-balancing.

You can configure the port priority in the following ways.

I. Configure in system view

Perform the following configuration in system view.

Table 1-16 Configure the port priority

Operation	Command
Configure the port priority.	**stp interface** *interface-list* [**instance** *instance-id*] **port priority** *priority*
Restore the default port priority.	**undo stp interface** *interface-list* [**instance** *instance-id*] **port priority**

II. Configure in Ethernet port view

Perform the following configuration in Ethernet port view.

Table 1-17 Configure the port priority

Operation	Command
Configure the port priority.	**stp** [**instance** *instance-id*] **port priority** *priority*
Restore the default port priority.	**undo stp** [**instance** *instance-id*] **port priority**

You can configure the port priority with either of the above-mentioned measures. For more about the commands, refer to the *Command Manual*.

Upon the change of port priority, MSTP will recalculate the port role and transit the state. Generally, a smaller value represents a higher priority. If all the Ethernet ports of a switch are configured with the same priority value, the priorities of the ports will be differentiated by the index number. The change of Ethernet port priority will lead to spanning tree recalculation. You can configure the port priority per actual networking requirements.

By default, the priority of all the Ethernet ports is 128.

1.2.12 Configure the Port (not) to Connect with the Point-to-Point Link

The point-to-point link directly connects two switches.

You can configure the port (not) to connect with the point-to-point link in the following ways.

I. Configure in system view

Perform the following configuration in system view.

Table 1-18 Configure the port (not) to connect with the point-to-point link

Operation	Command
Configure the port to connect with the point-to-point link.	**stp interface** *interface-list* **point-to-point force-true**
Configure the port not to connect with the point-to-point link.	**stp interface** *interface-list* **point-to-point force-false**
Configure MSTP to automatically detect if the port is directly connected with the point-to-point link.	**stp interface** *interface-list* **point-to-point auto**
Configure MSTP to automatically detect if the port is directly connected with the point-to-point link, as defaulted.	**undo stp interface** *interface-list* **point-to-point**

II. Configure in Ethernet port view

Perform the following configuration in Ethernet port view.

Table 1-19 Configure the port (not) to connect with the point-to-point link

Operation	Command
Configure the port to connect with the point-to-point link.	**stp point-to-point force-true**
Configure the port not to connect with the point-to-point link.	**stp point-to-point force-false**
Configure MSTP to automatically detect if the port is directly connected with the point-to-point link.	**stp point-to-point auto**
Configure MSTP to automatically detect if the port is directly connected with the point-to-point link, as defaulted.	**undo stp point-to-point**

You can configure the port (not) to connect with the point-to-point link with either of the above-mentioned measures. For more about the commands, refer to the *Command Manual*.

For the ports connected with the point-to-point link, upon some port role conditions met, they can transit to forwarding state fast through transmitting synchronization packet, thereby reducing the unnecessary forwarding delay. If the parameter is configured as auto mode, MSTP will automatically detect if the current Ethernet port is connected with the point-to-point link.

Note:

For a link aggregation, only the master port can be configured to connect with the point-to-point link. If a port in auto-negotiation mode operates in full-duplex mode upon negotiation, it can be configured to connect with the point-to-point link.

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 to which 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.

By default, the parameter is configured as **auto**.

1.2.13 Configure the mCheck Variable of a Port

The port of an MSTP switch operates in either STP-compatible or MSTP mode.

Suppose a port of an MSTP switch on a switching network is connected to an STP switch, the port will automatically transit to operate in STP-compatible mode. However, the port stays in STP-compatible mode and cannot automatically transit back to MSTP mode when the STP switch is removed. In this case, you can perform mCheck operation to transit the port to MSTP mode by force.

You can use the following measure to perform mCheck operation on a port.

I. Configure in system view

Perform the following configuration in system view.

Table 1-20 Configure the mCheck variable of a port

Operation	Command
Perform mCheck operation on a port.	**stp interface** *interface-list* **mcheck**

II. Configure in Ethernet port view

Perform the following configuration in Ethernet port view.

Table 1-21 Configure the mCheck variable of a port

Operation	Command
Perform mCheck operation on a port.	**stp mcheck**

You can configure mCheck variable on a port with either of the above-mentioned measures. For more about the commands, refer to the *Command Manual*.

Note that the command can be used only if the switch runs MSTP. The command does not make any sense when the switch runs in STP-compatible mode.

1.2.14 Configure the Switch Security Function

An MSTP switch provides BPDU protection , Root protection functions, loop protection and TC-protection .

I. BPDU protection

For an access device, the access port is generally directly connected to the user terminal (e.g., PC) or a file server, and the access port is set to edge port to implement fast transition. When such port receives BPDU packet, the system will automatically set it as a non-edge port and recalculate the spanning tree, which causes the network topology flapping. In normal case, these ports will not receive STP BPDU. If someone forges BPDU to attack the switch, the network will flap. BPDU protection function is used against such network attack.

II. Root protection

The primary and secondary root bridgees of the spanning tree, especially those of ICST, shall be located in the same region. It is because the primary and secondary roots of CIST are generally placed in the core region with a high bandwidth in network design. 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.

III. loop protection

The root port and other blocked ports maintain their state according to the BPDUs send by uplink switch. Once the link is blocked or has trouble, then the ports cannot receive BPDUs and the switch will select root port again. In this case, the former root port will turn into specified port and the former blocked ports will enter forwarding state, as a result, a link loop will be generated.

The security functions can control the generation of loop. After it is enabled, the root port cannot be changed, the blocked port will maintain in “Discarding” state and do not forward packets, thus to avoid link loop.

IV. TC-protection

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.

You can use the following command to configure the security functions of the switch.

Perform the following configuration in corresponding configuration modes.

Table 1-22 Configure the switch security function

Operation	Command
Configure switch BPDU protection (from system view)	**stp bpdu-protection**
Restore the disabled BPDU protection state as defaulted (from system view)	**undo stp bpdu-protection**
Configure switch Root protection (from system view)	**stp interface** *interface-list* **root-protection**
Restore the disabled Root protection state as defaulted (from system view)	**undo stp interface** *interface-list* **root-protection**
Configure switch Root protection (from Ethernet port view)	**stp root-protection**
Restore the disabled Root protection state as defaulted (from Ethernet port view)	**undo stp root-protection**
Configure switch loop protection function (from Ethernet port view)	**stp loop-protection**
Restore the disabled loop protection state, as defaulted (from Ethernet port view)	**stp loop-protection**
Configure switch TC protection (from system view)	**stp tc-protection enable**
Disabled TC protection state as defaulted (from system view)	**stp tc-protection disable**

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.

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.

When configure a port, only one configuration can be effective among loop protection, Root protection and Edge port configuration at same moment.

By default, the switch does not enable BPDU protection or Root protection.

By default, the protection from TC-BPDU packet attack is enabled.

For more about the configuration commands, refer to the *Command Manual*.

1.2.15 Enable MSTP on the Device

You can use the following command to enable MSTP on the device.

Perform the following configuration in system view.

Table 1-23 Enable/Disable MSTP on a device

Operation	Command
Enable MSTP on a device.	**stp enable**
Disable MSTP on a device.	**stp disable**
Restore the disable state of MSTP, as defaulted.	**undo stp**

Only if MSTP has been enabled on the device will other MSTP configurations take effect.

By default, MSTP is disabled.

1.2.16 Enable/Disable MSTP on a Port

You can use the following command to enable/disable MSTP on a port. You may disable MSTP on some Ethernet ports of a switch to spare them from spanning tree calculation. This is a measure to flexibly control MSTP operation and save the CPU resources of the switch.

MSTP can be enabled/disabled on a port through the following ways.

I. Configure in system view

Perform the following configuration in system view.

Table 1-24 Enable/Disable MSTP on a port

Operation	Command
Enable MSTP on a port.	**stp interface** *interface-list* **enable**
Disable MSTP on a port.	**stp interface** *interface-list* **disable**
Restore the default MSTP state on the port.	**undo stp** *interface-list*

II. Configure in Ethernet port view

Perform the following configuration in Ethernet port view.

Table 1-25 Enable/Disable MSTP on a port

Operation	Command
Enable MSTP on a port.	**stp enable**
Disable MSTP on a port.	**stp disable**
Restore the default MSTP state on the port.	**undo stp**

You can enable/disable MSTP on a port with either of the above-mentioned measures. For more about the commands, refer to the *Command Manual*.

Note that redundant route may be generated after MSTP is disabled.

By default, MSTP is enabled on all the ports after it is enabled on the device.

1.3 Display and Debug MSTP

After the above configuration, execute **display** command in any view to display the running of the MSTP configuration, and to verify the effect of the configuration. Execute **reset** command in user view to clear the statistics of MSTP module. Execute **debugging** command in user view to debug the MSTP module

Table 1-26 Display and Debug MSTP

Operation	Command
Show the configuration information about the current port and the switch.	**display stp** [**instance** *instance-id*] [**interface** *interface-list* | **slot** *slot-num*] [**brief**]
Show the configuration information about the region.	**display stp region-configuration**
Clear the MSTP statistics information.	**reset stp** [**interface** *interface-list*]
Enable/Disable MSTP (packet receiving/transmitting, event, error) debugging on the port.	[**undo**] **debugging stp** [**interface** *interface-list*] { **packet** | **event** }
Enable/Disable the global MSTP debugging.	[**undo**] **debugging stp** { **global-event** | **global-error** | **all** }
Enable/Disable specified STI debugging	[**undo**] **debugging stp instance** *instance-id*

HUAWEI

Quidway S3000-EI Series Ethernet Switches
Operation Manual

Security

Table of Contents

Chapter 1 802.1x Configuration

1.1 802.1x Overview

1.1.1 802.1x Standard Overview

IEEE 802.1x (hereinafter simplified as 802.1x) is a port-based network access control protocol that is used as the standard for LAN user access authentication.

In the LANs complying with the IEEE 802 standards, the user can access the devices and share the resources in the LAN through connecting the LAN access control device like the LAN Switch. However, in telecom access, commercial LAN (a typical example is the LAN in the office building) and mobile office etc., the LAN providers generally hope to control the user's access. In these cases, the requirement on the above-mentioned "Port Based Network Access Control" originates.

"Port Based Network Access Control" means to authenticate and control all the accessed devices on the port of LAN access control device. If the user's device connected to the port can pass the authentication, the user can access the resources in the LAN. Otherwise, the user cannot access the resources in the LAN. It equals that the user is physically disconnected.

802.1x defines port based network access control protocol and only defines the point-to-point connection between the access device and the access port. The port can be either physical or logical. The typical application environment is as follows: Each physical port of the LAN Switch only connects to one user workstation (based on the physical port) and the wireless LAN access environment defined by the IEEE 802.11 standard (based on the logical port), etc.

1.1.2 802.1x System Architecture

The system using the 802.1x is the typical C/S (Client/Server) system architecture. It contains three entities, which are illustrated in the following figure: Supplicant System, Authenticator System and Authentication Server System.

The LAN access control device needs to provide the Authenticator System of 802.1x. The devices at the user side such as the computers need to be installed with the 802.1x client Supplicant software, for example, the 802.1x client provided by Huawei Technologies Co., Ltd. (or by Microsoft Windows XP). The 802.1x Authentication Server system normally stays in the carrier's AAA center.

Authenticator and Authentication Server exchange information through EAP (Extensible Authentication Protocol) frames. The Supplicant and the Authenticator exchange information through the EAPoL (Extensible Authentication Protocol over LANs) frame defined by IEEE 802.1x. Authentication data are encapsulated in the EAP

frame, which is to be encapsulated in the packets of other AAA upper layer protocols (e.g. RADIUS) so as to go through the complicated network to reach the Authentication Server. Such procedure is called EAP Relay.

There are two types of ports for the Authenticator. One is the Uncontrolled Port, and the other is the Controlled Port. The Uncontrolled Port is always in bi-directional connection state. The user can access and share the network resources any time through the ports. The Controlled Port will be in connecting state only after the user passes the authentication. Then the user is allowed to access the network resources.

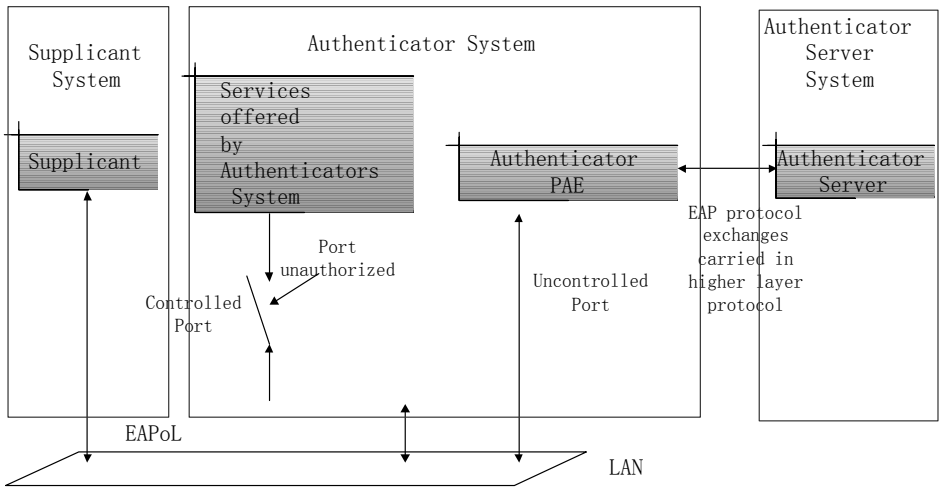


Figure 1-1 802.1x system architecture

1.1.3 802.1x Authentication Process

802.1x configures EAP frame to carry the authentication information. The Standard defines the following types of EAP frames:

- EAP-Packet: Authentication information frame, used to carry the authentication information.
- EAPoL-Start: Authentication originating frame, actively originated by the Supplicant.
- EAPoL-Logoff: Logoff request frame, actively terminating the authenticated state.
- EAPoL-Key: Key information frame, supporting to encrypt the EAP packets.
- EAPoL-Encapsulated-ASF-Alert: Supports the Alerting message of Alert Standard Forum (ASF).

The EAPoL-Start, EAPoL-Logoff and EAPoL-Key only exist between the Supplicant and the Authenticator. The EAP-Packet information is re-encapsulated by the Authenticator System and then transmitted to the Authentication Server System. The EAPoL-Encapsulated-ASF-Alert is related to the network management information and terminated by the Authenticator.

802.1x provides an implementation solution of user ID authentication. However, 802.1x itself is not enough to implement the scheme. The administrator of the access device should configure the AAA scheme by selecting RADIUS or local authentication so as to assist 802.1x to implement the user ID authentication. For detailed description of AAA, refer to the corresponding AAA configuration.

1.1.4 Implementing 802.1x on the Ethernet Switch

Quidway Series Ethernet Switches not only support the port access authentication method regulated by 802.1x, but also extend and optimize it in the following way:

- Support to connect several End Stations in the downstream via a physical port.
- The access control (or the user authentication method) can be based on port or MAC address.

In this way, the system becomes much securer and easier to manage.

1.2 Configuring 802.1x

The configuration tasks of 802.1x itself can be fulfilled in system view of the Ethernet switch. When the global 802.1x is not enabled, the user can configure the 802.1x state of the port. The configured items will take effect after the global 802.1x is enabled.

Note:

When 802.1x is enabled on a port, the max number of MAC address learning which is configured by the command **mac-address max-mac-count** cannot be configured on the port, and vice versa.

The Main 802.1x configuration includes:

- Enabling/disabling 802.1x
- Setting the port access control mode
- Setting the port access control method
- Checking the users that log on the switch via proxy
- Setting the maximum number of users via each port
- Setting the Authentication in DHCP Environment
- Configuring the authentication method for 802.1x user
- Enabling/Disabling Guest VLAN
- Setting 802.1x Re-authentication
- Setting 802.1x Client Version Authentication
- Configuring 802.1x dynamic user binding
- Setting the maximum times of authentication request message retransmission
- Configuring timers

- Enabling/disabling a quiet-period timer

Among the above tasks, the first one is compulsory, otherwise 802.1x will not take any effect. The other tasks are optional. You can perform the configurations at requirements.

1.2.1 Enabling/Disabling 802.1x

The following command can be used to enable/disable the 802.1x on the specified port or globally. When it is used in system view, if the parameter *interface-list* is not specified, 802.1x will be globally enabled. If the parameter *interface-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.

Perform the following configurations in system view or Ethernet port view.

Table 1-1 Enabling/disabling 802.1x

Operation	Command
Enable the 802.1x	**dot1x** [**interface** *interface-list*]
Disable the 802.1x	**undo dot1x** [**interface** *interface-list*]

You can configure 802.1x on individual port before it is enabled globally. The configuration will take effect right after 802.1x is enabled globally.

By default, 802.1x authentication has not been enabled globally and on any port.

1.2.2 Setting the Port Access Control Mode.

The following commands can be used for setting 802.1x access control mode on the specified port. When no port is specified, the access control mode of all ports is configured.

Perform the following configurations in system view or Ethernet port view.

Table 1-2 Setting the port access control mode.

Operation	Command
Set the port access control mode.	**dot1x port-control** { **authorized- force** | **unauthorized-force** | **auto** } [**interface** *interface-list*]
Restore the default access control mode of the port.	**undo dot1x port-control** [**interface** *interface-list*]

By default, the mode of 802.1x performing access control on the port is **auto** (automatic identification mode, which is also called protocol control mode). That is, the initial state

of the port is unauthorized. It only permits EAPoL packets receiving/transmitting and does not permit the user to access the network resources. If the authentication flow is passed, the port will be switched to the authorized state and permit the user to access the network resources. This is the most common case.

1.2.3 Setting the Port Access Control Method

The following commands are used for setting 802.1x access control method on the specified port. When no port is specified in system view, the access control method of port is configured globally.

Perform the following configurations in system view or Ethernet port view.

Table 1-3 Setting the port access control method

Operation	Command
Set port access control method	**dot1x port-method** { **macbased** | **portbased** } [**interface** *interface-list*]
Restore the default port access control method	**undo dot1x port-method** [**interface** *interface-list*]

By default, 802.1x authentication method on the port is **macbased**. That is, authentication is performed based on MAC addresses.

1.2.4 Checking the Users that Log on the Switch via Proxy

The following commands are used for checking the users that log on the switch via proxy.

Perform the following configurations in system view or Ethernet port view.

Table 1-4 Checking the users that log on the switch via proxy

Operation	Command
Enable the check for access users via proxy	**dot1x supp-proxy-check** { **logoff** | **trap** } [**interface** *interface-list*]
Cancel the check for access users via proxy	**undo dot1x supp-proxy-check** { **logoff** | **trap** } [**interface** *interface-list*]

These commands can be 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.

1.2.5 Setting the Supplicant Number on a Port

The following commands are used for setting number of users allowed by 802.1x on specified port. When no port is specified, all the ports accept the same number of supplicants.

Perform the following configurations in system view or Ethernet port view.

Table 1-5 Setting the maximum number of users via a specified port

Operation	Command
Set maximum number of users via specified port	**dot1x max-user** *user-number* [**interface** *interface-list*]
Restore the maximum number of users on the port to the default value	**undo dot1x max-user** [**interface** *interface-list*]

By default, 802.1x allows up to 256 supplicants on each port for S3000-EI Series Ethernet switches.

1.2.6 Setting the Authentication in DHCP Environment

If in DHCP environment the users configure static IP addresses, you can set 802.1x to disable the switch to trigger the user ID authentication over them with the following command.

Perform the following configurations in system view.

Table 1-6 Setting the Authentication in DHCP Environment

Operation	Command
Disable the switch to trigger the user ID authentication over the users who configure static IP addresses in DHCP environment	**dot1x dhcp-launch**
Enable the switch to trigger the authentication over them	**undo dot1x dhcp-launch**

By default, the switch can trigger the user ID authentication over the users who configure static IP addresses in DHCP environment.

1.2.7 Configuring the Authentication Method for 802.1x User

The following commands can be used to configure the authentication method for 802.1x user. Three kinds of methods are available: PAP authentication (RADIUS server must support PAP authentication), CHAP authentication (RADIUS server must support CHAP authentication), EAP relay authentication (switch send authentication

information to RADIUS server in the form of EAP packets directly and RADIUS server must support EAP authentication).

For EAP authentication, PEAP, EAP-TLS and EAP-MD5 methods are available on the switch:

- EAP-TLS: The client and RADIUS server check in EAP-TLS approach mutually the security certificate authority of the other's, to guarantee the validity of the certificates and prevent data from being illegally used.
- PEAP: As a kind of EAP protocol, protected EAP (PEAP) first establishes an encrypted transport layer security (TLS) channel to provide integrity protection, and then initiates a new type of EAP negotiation, to accomplish identity authentication to the client.

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.

Perform the following configurations in system view.

Table 1-7 Configuring the authentication method for 802.1x user

Operation	Command
Configure authentication method for 802.1x user	**dot1x authentication-method** { **chap** | **pap** | **eap** }
Restore the default authentication method for 802.1x user	**undo dot1x authentication-method**

By default, CHAP authentication is used for 802.1x user authentication.

1.2.8 Enabling/Disabling Guest VLAN

After the Guest VLAN function is enabled, the switch broadcasts active authentication packets to all ports on which 802.1x are enabled. If there is still some ports do not return response packets after being re-authenticated for maximum times, the switch adds this ports into Guest VLAN. After that, no 802.1x authentication is performed when the user of the Guest VLAN visits the resources within this Guest VLAN. However, if the user visits the outer resources, authentication is still needed. In this way, the requirements of allowing unauthenticated users to access some resources are met, such as, the user accesses some resources without installing 802.1x client, or the user upgrades 802.1x client without authentication, and so on.

Perform the following configuration in system view or Ethernet port view.

Table 1-8 Enabling/disabling Guest VLAN

Operation	Command
Enabling Guest VLAN	**dot1x guest-vlan** *vlan-id* [**interface** *interface-list*]
Disabling Guest VLAN	**undo dot1x guest-vlan** *vlan-id* [**interface** *interface-list*]

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 **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.

1.2.9 Setting 802.1x Re-authentication

If the termination-action attribute on the RADIUS server is set to 1, the server then sets the termination-action attribute in the access-accept packet which is sent to the switch to 1. The switch re-authenticates the access user periodically after receiving this kind of packets.

You can also enable 802.1x re-authentication on the switch through this configuration, making the switch re-authenticates the access users periodically.

I. Enabling 802.1x re-authentication

Before enabling the 802.1x re-authentication, you must enable the 802.1x feature both on the port and globally.

Perform the following in system view or Ethernet port view.

Table 1-9 Enabling/disabling 802.1x user re-authentication

Operation	Command
Enable 802.1x user re-authentication	**dot1x re-authenticate** [**interface** *interface-list*]
Disable 802.1x user re-authentication	**undo dot1x re-authenticate** [**interface** *interface-list*]

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.

II. Configuring 802.1x re-authentication timeout timer

The period of re-authentication is decided by the following two modes:

1) The switch takes the session-timeout value in the access-accept packet as the authentication period.
2) The switch takes the value set by the user through the **dot1x reauth-period** command as the authentication period. And this period defaults to 3600 seconds.

During the authentication, the switch takes the last received one as the authentication period. For example, after the user configured the authentication period on the switch, the switch receives the packet with the termination-action attributes of 1, and then the switch takes the session-timeout value in the access-accept packet as the authentication period.

Perform the following in system view.

Table 1-10 Configuring 802.1x re-authentication timeout timer

Operation	Command
Configure parameters of the timer	**dot1x timer reauth-period** *reauth-period-value*
Return to the defaults	**undo dot1x timer reauth-period**

By default, *reauth-period-value* is 3600 seconds.

1.2.10 Setting 802.1x Client Version Authentication

After enabling 802.1x client version authentication, the switch authenticates the version and validity of the 802.1x client of the access user, avoiding the access of the users at the client with the defectively old version or at the invalid client.

I. Enabling 802.1x client version authentication

Perform the following in system view or Ethernet port view.

Table 1-11 Setting 802.1x client version authentication

Operation	Command
Enable 802.1x client version authentication	**dot1x version-check** [**interface** *interface-list*]
Disable 802.1x client version authentication	**undo dot1x version-check** [**interface** *interface-list*]

By default, 802.1x client version 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 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.

II. Configuring the maximum retry times for the switch to send version request frame to the client

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.

Perform the following in system view.

Table 1-12 Configuring the maximum retry times for the switch to send version request frame to the client

Operation	Command
Configure the maximum retry times for the switch to send version request frame to the client	**dot1x retry-version-max** *max-retry-version-value*
Return to the defaults	**undo dot1x retry-version-max**

By default, the switch tries 3 times at the most to send version request frame to the access user.

III. Configuring the timeout timer of version authentication

Perform the following in system view.

Table 1-13 Configuring the timeout timer of version authentication

Operation	Command
Configure parameters of the timer	**dot1x timer ver-period** *ver-period-value*
Return to the defaults	**undo dot1x timer ver-period**

By default, *ver-period-value* is 1 second.

1.2.11 Configuring 802.1x Dynamic User Binding

I. Overview

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.

Dynamic user binding can be used to:

- Prevent users from changing their IP addresses. As some kind of accounting servers charge by IP addresses, changing of IP addresses causes these accounting servers failing to charge effectively.
- Prevent unauthenticated user from accessing a network through authentication ports when in port-based authentication mode. With dynamic user binding disabled, port-based authentication mode enables other users to access the network without being authenticated after a user passes the authentication. Whereas when dynamic user binding is enabled, a switch binds the corresponding IP address, the MAC address, the accessing port, and the VLAN to which the accessing port belongs after a user passes the authentication, which prevents other users from accessing the network through the port.

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, you 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.

II. Configuration Prerequisites

- Enable 802.1x feature globally and on a port.
- If you obtain an IP address dynamically, enable DHCP Snooping globally on the switch and configure the switch port connecting to the DHCP server to be a DHCP Snooping trusted port.

III. Configuration Procedure

Table 1-14 Configure 802.1x dynamic user binding

Operation	Command	Remarks
Enter system view	**system-view**	—
Enable 802.1x dynamic user binding	**dot1x dynamic-binding-user enable**	Required. 802.1x dynamic user binding is disabled by default.
Display related information	**display dot1x** [**sessions** | **statistics**] [**interface** *interface-list*]	The **display** command can be executed in any view.

IV. 802.1x Dynamic User Binding Configuration Example

1) Network requirements

- The 802.1x users obtain IP addresses dynamically.
- Configure the switch to prevent 802.1x users from changing their IP addresses after they pass the authentication.

2) Configuration procedure

Enable 802.1x globally.

```
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] dot1x
```

Enable 802.1x dynamic user binding.

```
[Quidway] dot1x dynamic-binding-user enable
```

Enable DHCP Snooping globally. (Required for 802.1x users who obtain IP addresses dynamically)

```
[Quidway] dhcp-snooping
```

Configure Ethernet 0/1 port, which connects the DHCP server, to be a DHCP Snooping trusted port. (Required for 802.1x users who obtain IP addresses dynamically)

```
[Quidway] interface ethernet0/1
[Quidway-Ethernet0/1] dhcp-snooping trust
```

1.2.12 Setting the Maximum Times of Authentication Request Message Retransmission

The following commands are used for setting the maximum retransmission times of the authentication request message that the switch sends to the supplicant.

Perform the following configurations in system view.

Table 1-15 Setting the maximum times of the authentication request message retransmission

Operation	Command
Set the maximum times of the authentication request message retransmission	**dot1x retry** *max-retry-value*
Restore the default maximum retransmission times	**undo dot1x retry**

By default, the *max-retry-value* is 3. That is, the switch can retransmit the authentication request message to a supplicant for 3 times at most.

1.2.13 Configuring Timers

The following commands are used for configuring the 802.1x timers.

Perform the following configurations in system view.

Table 1-16 Configuring timers

Operation	Command
Configure timers	**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* }
Restore default settings of the timers	**undo dot1x timer** { **handshake-period** | **quiet-period** | **reauth-period** | **server-timeout** | **supp-timeout** | **tx-period** | **ver-period** }

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.

1.2.14 Enabling/Disabling a Quiet-Period Timer

You can use the following commands to enable/disable a quiet-period timer of an Authenticator (which can be a Quidway Series Ethernet Switch). If an 802.1x user has not passed the authentication, the Authenticator will keep quiet for a while (which is specified by **dot1x timer quiet-period** command) before launching the authentication again. During the quiet period, the Authenticator does not do anything related to 802.1x authentication.

Perform the following configuration in system view.

Table 1-17 Enabling/disabling a quiet-period timer

Operation	Command
Enable a quiet-period timer	**dot1x quiet-period**
Disable a quiet-period timer	**undo dot1x quiet-period**

By default, **quiet-period** timer is disabled.

1.3 Displaying and Debugging 802.1x

After the above configuration, execute **display** command in any view to display the running of the VLAN configuration, and to verify the effect of the configuration. Execute **reset** command in user view to reset 802.1x statistics. Execute **debugging** command in user view to debug 802.1x.

Table 1-18 Displaying and debugging 802.1x

Operation	Command
Display the configuration, running and statistics information of 802.1x	**display dot1x** [**sessions** | **statistics**] [**interface** *interface-list*]
Reset the 802.1x statistics information	**reset dot1x statistics** [**interface** *interface-list*]
Enable the error/event/packet/all debugging of 802.1x	**debugging dot1x** { **error** | **event** | **packet** | **all** }
Disable the error/event/packet/all debugging of 802.1x.	**undo debugging dot1x** { **error** | **event** | **packet** | **all** }

1.4 802.1x Configuration Example

I. Networking requirements

As shown in the following figure, the workstation of a user is connected to the port Ethernet 0/1 of the Switch.

The switch administrator will enable 802.1x on all the ports to authenticate the supplicants so as to control their access to the Internet. The access control mode is configured as based on the MAC address

All the supplicants belong to the default domain huawei163.net, which can contain up to 30 users. RADIUS authentication is performed first. If there is no response from the RADIUS server, local authentication will be performed. For accounting, if the RADIUS server fails to account, the user will be disconnected. In addition, when the user is accessed, the domain name does not follow the user name. Normally, if the user's traffic is less than 2kbps consistently over 20 minutes, he will be disconnected.

A server group, consisting of two RADIUS servers at 10.11.1.1 and 10.11.1.2 respectively, is connected to the switch. The former one acts as the primary-authentication/secondary-accounting server. The latter one acts as the primary-accounting server. Set the encryption key as “name” when the system exchanges packets with the authentication RADIUS server and “money” when the system exchanges packets with the accounting RADIUS server. Configure the system to retransmit packets to the RADIUS server if no response received in 5 seconds. Retransmit the packet no more than 5 times in all. Configure the system to transmit a real-time accounting packet to the RADIUS server every 15 minutes. The system is instructed to transmit the user name to the RADIUS server after removing the user domain name.

The user name of the local 802.1x access user is localuser and the password is localpass (input in plain text). The idle cut function is enabled.

II. Networking diagram

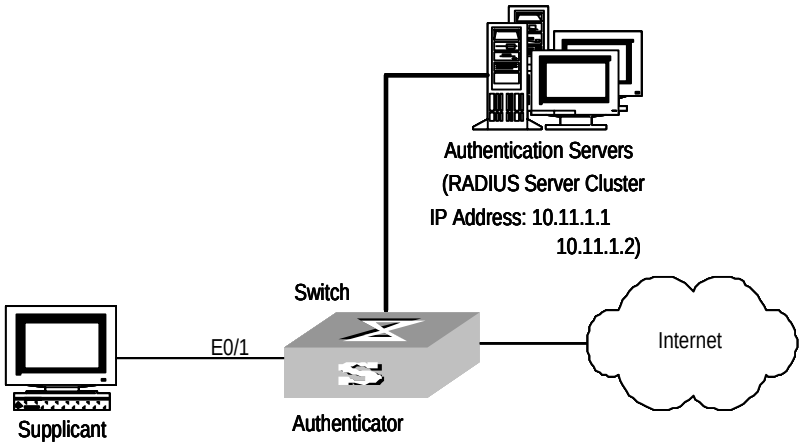


Figure 1-2 Enabling 802.1x and RADIUS to perform AAA on the supplicant

III. Configuration procedure

Note:

The following examples concern most of the AAA/RADIUS configuration commands. For details, refer to the chapter AAA and RADIUS Protocol Configuration.
The configurations of accessing user workstation and the RADIUS server are omitted.

Enable the 802.1x performance on the specified port Ethernet 0/1.

```
[Quidway] dot1x interface Ethernet 0/1
```

Set the access control mode. (This command could not be configured, when it is configured as MAC-based by default.)

```
[Quidway] dot1x port-method macbased interface Ethernet 0/1
```

Create the RADIUS scheme radius1 and enters its view.

```
[Quidway] radius scheme radius1
```

Set IP address of the primary authentication/accounting RADIUS servers.

```
[Quidway-radius-radius1] primary authentication 10.11.1.1
[Quidway-radius-radius1] primary accounting 10.11.1.2
```

Set the IP address of the second authentication/accounting RADIUS servers.

```
[Quidway-radius-radius1] secondary authentication 127.0.0.1 1645
[Quidway-radius-radius1] secondary accounting 10.11.1.1
[Quidway-radius-radius1] quit
```

Set the encryption key when the system exchanges packets with the authentication RADIUS server.

```
[Quidway] local-server nas-ip 127.0.0.1 key name
[Quidway] radius scheme radius1
[Quidway-radius-radius1] key authentication name
```

Set the encryption key when the system exchanges packets with the accounting RADIUS server.

```
[Quidway-radius-radius1] key accounting money
```

Set the timeouts and times for the system to retransmit packets to the RADIUS server.

```
[Quidway-radius-radius1] timer 5
[Quidway-radius-radius1] retry 5
```

Set the interval for the system to transmit real-time accounting packets to the RADIUS server.

```
[Quidway-radius-radius1] timer realtime-accounting 15
```

Configure the system to transmit the user name to the RADIUS server after removing the domain name.

```
[Quidway-radius-radius1] user-name-format without-domain
[Quidway-radius-radius1] quit
```

Create the user domain huawei163.net and enters isp configuration mode.

```
[Quidway] domain huawei163.net
```

Specify radius1 as the RADIUS scheme for the users in the domain huawei163.net.

```
[Quidway-isp-huawei163.net] radius-scheme radius1
```

Set a limit of 30 users to the domain huawei163.net.

```
[Quidway-isp-huawei163.net] access-limit enable 30
```

Enable idle cut function for the user and set the idle cut parameter in the domain huawei163.net.

```
[Quidway-isp-huawei163.net] idle-cut enable 20 2000
```

Add a local supplicant and sets its parameter.

```
[Quidway] local-user localuser
[Quidway-luser-localuser] service-type lan-access
[Quidway-luser-localuser] password simple localpass
```

Enable the 802.1x globally.

```
[Quidway] dot1x
```

Chapter 2 AAA and RADIUS Protocol Configuration

2.1 AAA and RADIUS Protocol Overview

2.1.1 AAA Overview

Authentication, Authorization and Accounting (AAA) provide a uniform framework used for configuring these three security functions to implement the network security management.

The network security mentioned here refers to access control and it includes:

- Which user can access the network server?
- Which service can the authorized user enjoy?
- How to keep accounts for the user who is using network resource?

Accordingly, AAA shall provide the following services:

- Authentication: authenticates if the user can access the network server.
- Authorization: authorizes the user with specified services.
- Accounting: traces network resources consumed by the user.

Generally applying Client/Server architecture, in which client ends run as managed sources and the servers centralize and store user information, AAA framework owns the good scalability, and is easy to realize the control and centralized management of user information.

2.1.2 RADIUS Protocol Overview

As mentioned above, AAA is a management framework, so it can be implemented by some protocols. RADIUS is such a protocol frequently used.

I. What is RADIUS

Remote Authentication Dial-In User Service, RADIUS for short, is a kind of distributed information switching protocol in Client/Server architecture. RADIUS can prevent the network from interruption of unauthorized access and it is often used in the network environments requiring both high security and remote user access. For example, it is often used for managing a large number of scattering dial-in users who use serial ports and modems. RADIUS system is the important auxiliary part of Network Access Server (NAS).

After RADIUS system is started, if the user wants to have right to access other network or consume some network resources through connection to NAS (dial-in access server

in PSTN environment or Ethernet switch with access function in Ethernet environment), NAS, namely RADIUS client end, will transmit user AAA request to the RADIUS server. RADIUS server has a user database recording all the information of user authentication and network service access. When receiving user's request from NAS, RADIUS server performs AAA through user database query and update and returns the configuration information and accounting data to NAS. Here, NAS controls supplicant and corresponding connections, while RADIUS protocol regulates how to transmit configuration and accounting information between NAS and RADIUS.

NAS and RADIUS exchange the information with UDP packets. During the interaction, both sides encrypt the packets with keys before uploading user configuration information (like password etc.) to avoid being intercepted or stolen.

II. RADIUS operation

RADIUS server generally uses proxy function of the devices like access server to perform user authentication. The operation process is as follows: First, the user send request message (the client username and encrypted password is included in the message) to RADIUS server. Second, the user will receive from RADIUS server various kinds of response messages in which the ACCEPT message indicates that the user has passed the authentication, and the REJECT message indicates that the user has not passed the authentication and needs to input username and password again, otherwise he will be rejected to access.

2.1.3 Implementing AAA/RADIUS on Ethernet Switch

By now, we understand that in the above-mentioned AAA/RADIUS framework, Quidway Series Ethernet Switches, serving as the user access device or NAS, is the client end of RADIUS. In other words, the AAA/RADIUS concerning client-end is implemented on Quidway Series Ethernet Switches. The figure below illustrates the RADIUS authentication network including Quidway Series Ethernet Switches.

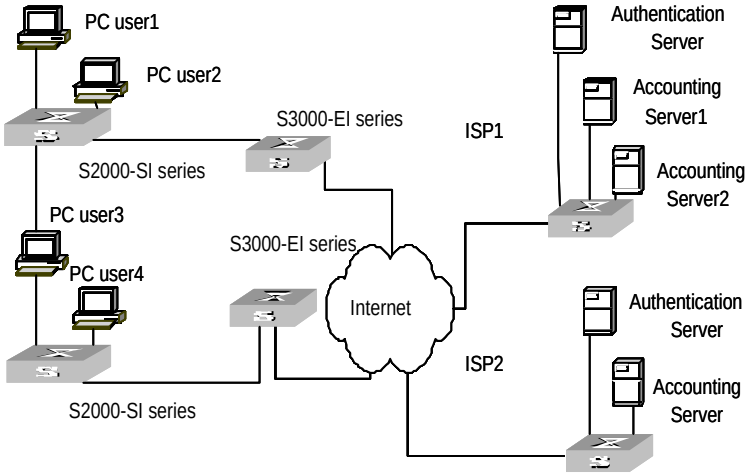


Figure 2-1 Networking when S3000-EI Series Ethernet Switches applying RADIUS authentication

2.2 AAA Configuration

AAA configuration includes:

- Creating/Deleting ISP Domain
- Configuring Relevant Attributes of ISP Domain
- Enabling/Disabling the Messenger Alert
- Configuring Self-Service Server URL
- Creating a local user
- Setting attributes of local user
- Disconnecting a user by force
- Configuring Dynamic VLAN with RADIUS Server

Among the above configuration tasks, creating ISP domain is compulsory, otherwise the supplicant attributes cannot be distinguished. The other tasks are optional. You can configure them at requirements.

2.2.1 Creating/Deleting ISP Domain

What is Internet Service Provider (ISP) domain? To make it simple, 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 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 multi-ISP application environment. In such environment, one access device might access users of different ISP. Because the attributes of ISP users, such as username and password formats, etc,

may be different, it is necessary to differentiate them through setting ISP domain. In Quidway Series Switches ISP domain view, you can configure a complete set of exclusive ISP domain attributes on a per-ISP domain basis, which includes AAA policy (RADIUS scheme applied etc.)

For Quidway Series Switches, each supplicant belongs to an ISP domain. Up to 16 domains can be configured in the system. If a user has not reported its ISP domain name, the system will put it into the default domain.

Perform the following configurations in system view.

Table 2-1 Creating/Deleting ISP domain

Operation	Command
Create ISP domain or enter the view of a specified domain.	**domain** *isp-name*
Remove a specified ISP domain	**undo domain** *isp-name*
Enable the default ISP domain specified by *isp-name*	**domain default enable** *isp-name*
Restore the default ISP domain to “system”	**domain default disable**

By default, a domain named “system” has been created in the system. The attributes of “system” are all default values.

2.2.2 Configuring Relevant Attributes of ISP Domain

The relevant attributes of ISP domain include the adopted RADIUS scheme, state, and maximum number of supplicants . Where,

- The adopted RADIUS scheme is the one used by all the users in the ISP domain. The RADIUS scheme can be used for RADIUS authentication or accounting. By default, the default RADIUS scheme is used. The command shall be used together with the commands of setting RADIUS server and server cluster. For details, refer to the following Configuring RADIUS section of this chapter.
- Every ISP has active/block states. If an ISP domain is in active state, 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 already online. An ISP is in the block state when it is created. No user in the domain is allowed to request for network service.
- Maximum number of supplicants specifies how many supplicants can be contained in the ISP. For any ISP domain, there is no limit to the number of supplicants by default.
- The idle cut function means: If the traffic from a certain connection is lower than the defined traffic, cut off this connection.
- Perform the following configurations in ISP domain view.

Table 2-2 Configuring relevant attributes of ISP domain

Operation	Command
Specify the adopted RADIUS scheme	**radius-scheme** *radius-scheme-name*
Restore the adopted RADIUS scheme to the default RADIUS scheme	**undo radius-scheme**
Specify the ISP domain state to be used	**state** { **active** | **block** }
Set a limit to the amount of supplicants	**access-limit** { **disable** | **enable** *max-user-number* }
Restore the limit to the default setting	**undo access-limit**
Set the idle	**idle-cut** { **disable** | **enable** *minute* flow }

By default, after an ISP domain is created, the used RADIUS scheme is the default one named “system” (for relevant parameter configuration, refer to the Configuring RADIUS section of this chapter).,the state of domain is **active** , there is no limit to the amount of supplicants ,and the idle-cut function is disabled.

2.2.3 Enabling/Disabling the Messenger Alert

Messenger alert 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 following 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 updated remaining online time through a dialog box.

Perform the following configuration in ISP domain view.

Table 2-3 Enabling/disabling message alert

Operation	Command
Enable messenger alert and configure the remaining-online-time threshold and the interval at which the alert message is sent	**messenger time enable** *limit interval*
Disable messenger alert	**messenger time disable**
Restore the messenger alert as the default setting	**undo messenger time**

By default, messenger alert is disabled on the switch.

2.2.4 Configuring Self-Service Server URL

The **self-service-url enable** command can be used to configure self-service server uniform resource locator (URL). This command must be incorporated with a RADIUS 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.

Perform the following configuration in ISP domain view.

Table 2-4 Configuring the self-service server URL

Operation	Command
Configure self-service server URL and configure the URL address used to change the user password on the self-service server	**self-service-url enable** *url-string*
Remove the configuration of self-service server URL	**self-service-url disable**

By default, self-service server URL is not configured on the switch.

Note that, if "?" is contained in the URL, you must replace it with "|" when inputting the URL in the command line.

The "Change user password" option is available only when the user passes the authentication; otherwise, this option is in grey and unavailable.

2.2.5 Creating a Local User

A local user is a group of users set on NAS. The username is the unique identifier of a user. A supplicant requesting network service may use local authentication only if its corresponding local user has been added onto NAS.

Perform the following configurations in system view

Table 2-5 Creating/Deleting a local user and relevant properties

Operation	Command
Add local users	**local-user** *user-name*
Delete all the local users	**undo local-user all**
Delete a local user by specifying its type	**undo local-user** { *user-name* | **all** [**service-type** { **lan-access** | **ftp** | **telnet** | **ssh** }] }

By default, there is no local user in the system.

2.2.6 Setting Attributes of Local User

The attributes of a local user include its password display mode, state, service type and some other settings.

I. Setting the password display mode

Perform the following configurations in system view.

Table 2-6 Setting the method that a local user uses to display password

Operation	Command
Set the mode that a local user uses to display password	**local-user password-display-mode** { **cipher-force** | **auto** }
Cancel the mode that the local user uses to display password	**undo local-user password-display-mode**

Where, **auto** means that the password display mode will be the one specified by the user at the time of configuring password (see the **password** command in the following table for reference), and **cipher-force** means that the password display mode of all the accessing users must be in cipher text.

II. Setting the attributes of local users

Perform the following configurations in local user view.

Table 2-7 Setting/Removing the attributes concerned with a specified user

Operation	Command
Set a password for a specified user	**password** { **simple** | **cipher** } *password*
Remove the password set for the specified user	**undo password**
Set the state of the specified user	**state** { **active** | **block** }

Operation	Command
Set a service type for the specified user	**service-type** { **ftp** [**ftp-directory** *directory*] | **lan-access** | { **ssh** | **telnet** }* [**level** *level*] }
Cancel the service type of the specified user	**undo service-type** { **ftp** [**ftp-directory**] | **lan-access** | { **ssh** | **telnet** }* [**level**] }
Configure the attributes of lan-access users	**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* }*
Remove the attributes defined for the lan-access users	**undo attribute** { **ip** | **mac** | **idle-cut** | **access-limit** | **vlan** | **location** }*

2.2.7 Disconnecting a User by Force

Sometimes it is necessary to disconnect a user or a category of users by force. The system provides the following command to serve for this purpose.

Perform the following configurations in system view.

Table 2-8 Disconnecting a user by force

Operation	Command
Disconnect a user by force	**cut connection** { **all** | **access-type dot1x** } | **domain** *domain-name* | **interface** *portnum* | **ip** *ip-address* | **mac** *mac-address* | **radius-scheme** *radius-scheme-name* | **vlan** *vlanid* | **ucibindex** *ucib-index* | **user-name** *user-name* }

By default, no online user will be disconnected by force.

2.2.8 Configuring Dynamic VLAN with RADIUS Server

Based on the delivery attribute value of the RADIUS server, the switch adds the ports of the users who have passed the authentication to different VLANs, for purpose of controlling the network resources that the users can access. In the practical applications, the ports are set in port-based mode in order to work together with Guest VLAN. When the port is in MAC address-based mode, each port can only connect a single user.

Currently the ethernet switches support 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.

Note:

- For the string delivery mode, the VLAN to be delivered must be an existing one on the switch. That is, you must have created the VLAN and configured a name for it on the switch. There is no such a restriction for the integer mode.
- 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.

The dynamic VLAN with RADIUS server configuration includes:

- Configuring VLAN delivery mode
- Configuring name of the delivered VLAN

I. Configuring VLAN delivery mode

Perform the following configuration in ISP domain view.

Table 2-9 Configuring VLAN delivery mode

Operation	Command
Configure VLAN delivery mode as integer	**vlan-assignment-mode integer**
Configure VLAN delivery mode as string	**vlan-assignment-mode string**

By default, the integer mode is selected, that is, the switch supports the RADIUS server delivering the integer VLAN ID.

II. Configuring name of the delivered VLAN

Perform the following configuration in VLAN view.

Table 2-10 Configuring name of the delivered VLAN

Operation	Command
Configure name of the delivered VLAN	**name** *string*
Remove the configured VLAN name	**undo name**

2.3 Configuring RADIUS Protocol

For the Quidway Series Switches, the RADIUS protocol is configured on the per RADIUS scheme basis. In real networking environment, a RADIUS scheme can be an independent RADIUS server or a set of primary/second RADIUS servers with the same configuration but two different IP addresses. Accordingly, attributes of every RADIUS scheme include IP addresses of primary and second servers, shared key and RADIUS server type etc.

Actually, RADIUS protocol configuration only defines some necessary parameters using for information interaction between NAS and RADIUS Server. To make these parameters effective, it is necessary to configure, in the view, an ISP domain to use the RADIUS scheme and specify it to use RADIUS AAA schemes. For more about the configuration commands, refer to the AAA Configuration section above.

RADIUS protocol configuration includes:

- Creating/Deleting a RADIUS scheme
- Setting IP Address and Port Number of RADIUS Server
- Setting RADIUS packet encryption key
- Setting response timeout timer of RADIUS server
- Setting retransmission times of RADIUS request packet
- Enabling the selection of RADIUS accounting option
- Setting a real-time accounting interval
- Setting maximum times of real-time accounting request failing to be responded
- Enabling/Disabling stopping accounting request buffer
- Setting the maximum retransmitting times of stopping accounting request
- Setting the Supported Type of RADIUS Server
- Setting RADIUS server state
- Setting username format transmitted to RADIUS server
- Setting the unit of data flow that transmitted to RADIUS server
- Setting local RADIUS authentication server

Among the above tasks, creating RADIUS scheme and setting IP address of RADIUS server are required, while other takes are optional and can be performed as per your requirements.

2.3.1 Creating/Deleting a RADIUS scheme

As mentioned above, RADIUS protocol configurations are performed on the per RADIUS scheme basis. Therefore, before performing other RADIUS protocol configurations, it is compulsory to create the RADIUS scheme and enter its view to set its IP address.

You can use the following commands to create/delete a RADIUS scheme.

Perform the following configurations in system view.

Table 2-11 Creating/Deleting a RADIUS scheme

Operation	Command
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*
Delete a RADIUS scheme	**undo radius scheme** *radius-scheme-name*

Several ISP domains can use a RADIUS scheme at the same time. You can configure up to 16 RADIUS schemes, including the default scheme named as system.

By default, the system has a RADIUS scheme named “system” whose attributes are all default values. The default attribute values will be introduced in the following text.

2.3.2 Setting IP Address and Port Number of RADIUS Server

After creating a RADIUS scheme, you are supposed to set IP addresses and UDP port numbers for the RADIUS servers, including primary/second authentication/authorization servers and accounting servers. So you can configure up to 4 groups of IP addresses and UDP port numbers. However, at least you have to set one group of IP address and UDP port number for each pair of primary/second servers to ensure the normal AAA operation.

You can use the following commands to configure the IP address and port number for RADIUS servers.

Perform the following configurations in RADIUS scheme view.

Table 2-12 Setting IP Address and Port Number of RADIUS Server

Operation	Command
Set IP address and port number of primary RADIUS authentication/authorization server.	**primary authentication** *ip-address* [*port-number*]
Restore IP address and port number of primary RADIUS authentication/authorization or server to the default values.	**undo primary authentication**
Set IP address and port number of primary RADIUS accounting server.	**primary accounting** *ip-address* [*port-number*]
Restore IP address and port number of primary RADIUS accounting server or server to the default values.	**undo primary accounting**
Set IP address and port number of secondary RADIUS authentication/authorization server.	**secondary authentication** *ip-address* [*port-number*]
Restore IP address and port number of second RADIUS authentication/authorization or server to the default values.	**undo secondary authentication**

Operation	Command
Set IP address and port number of second RADIUS accounting server.	**secondary accounting** *ip-address* [*port-number*]
Restore IP address and port number of second RADIUS accounting server or server to the default values.	**undo secondary accounting**

In real networking environments, the above parameters shall be set according to the specific requirements. For example, you may specify 4 groups of different data to map 4 RADIUS servers, or specify one of the two servers as primary authentication/authorization server and second accounting server and the other one as second authentication/authorization server and primary accounting server, or you may also set 4 groups of exactly same data so that every server serves as a primary and second AAA server.

To guarantee the normal interaction between NAS and RADIUS server, you are supposed to guarantee the normal routes between RADIUS server and NAS before setting IP address and UDP port of the RADIUS server. In addition, because RADIUS protocol uses different UDP ports to receive/transmit authentication/authorization and accounting packets, you shall set two different ports accordingly. Suggested by RFC2138/2139, authentication/authorization port number is 1812 and accounting port number is 1813. However, you may use values other than the suggested ones. (Especially for some earlier RADIUS Servers, authentication/authorization port number is often set to 1645 and accounting port number is 1646.)

The RADIUS service port settings on Quidway Series Switches are supposed to be consistent with the port settings on RADIUS server. Normally, RADIUS accounting service port is 1813 and the authentication/authorization service port is 1812.

By default, all the IP addresses of primary/second authentication/authorization and accounting servers are 0.0.0.0, authentication/authorization service port is 1812 and accounting service UDP port is 1813.

2.3.3 Setting RADIUS Packet Encryption 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 to accept the packets from each other end and give response.

You can use the following commands to set the encryption key for RADIUS packets.

Perform the following configurations in RADIUS scheme view.

Table 2-13 Setting RADIUS packet encryption key

Operation	Command
Set RADIUS authentication/authorization packet encryption key	**key authentication** *string*
Restore the default RADIUS authentication/authorization packet encryption key.	**undo key authentication**
Set RADIUS accounting packet key	**key accounting** *string*
Restore the default RADIUS accounting packet key	**undo key accounting**

By default, the keys of RADIUS authentication/authorization and accounting packets are all “huawei”.

2.3.4 Setting Response Timeout Timer of RADIUS Server

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 request to guarantee RADIUS service for the user.

You can use the following command to set response timeout timer of RADIUS server.

Perform the following configurations in RADIUS scheme view.

Table 2-14 Setting response timeout timer of RADIUS server

Operation	Command
Set response timeout timer of RADIUS server	**timer** *seconds*
Restore the response timeout timer of RADIUS server to default value	**undo timer**

By default, timeout timer of RADIUS server is 3 seconds.

2.3.5 Setting Retransmission Times of RADIUS Request Packet

Since RADIUS protocol uses UDP packet to carry the data, the communication process is not reliable. If the RADIUS server has not responded NAS before 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.

You can use the following command to set retransmission times of RADIUS request packet.

Perform the following configurations in RADIUS scheme view.

Table 2-15 Setting retransmission times of RADIUS request packet

Operation	Command
Set retransmission times of RADIUS request packet	**retry** *retry-times*
Restore the default value of retransmission times	**undo retry**

By default, RADIUS request packet will be retransmitted up to three times.

2.3.6 Enabling The Selection Of Radius Accounting Option

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.

Perform the following configurations in RADIUS scheme view.

Table 2-16 Enabling the selection of RADIUS accounting option

Operation	Command
Enable the selection of RADIUS accounting option	**accounting optional**
Disable the selection of RADIUS accounting option	**undo accounting optional**

The user configured with **accounting optional** command in RADIUS scheme will no longer send real-time accounting update packet or offline accounting packet.

The **accounting optional** command in RADIUS scheme view is only effective on the accounting that uses this RADIUS scheme.

By default, selection of RADIUS accounting option is disabled.

2.3.7 Setting a Real-time Accounting 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.

You can use the following command to set a real-time accounting interval.

Perform the following configurations in RADIUS scheme view.

Table 2-17 Setting a real-time accounting interval

Operation	Command
Set a real-time accounting interval	**timer realtime-accounting** *minutes*
Restore the default value of the interval	**undo timer realtime-accounting**

The parameter *minutes* specifies the real-time accounting interval in minutes. The value shall be a multiple of 3.

The value of *minutes* is related to the performance of NAS and RADIUS server. The smaller the value is, the higher the performances of NAS and RADIUS are required. When there are a large amount of users (more than 1000, inclusive), we suggest a larger value. The following table recommends the ratio of *minute* value to the number of users.

Table 2-18 Recommended ratio of *minutes* to number of users

Number of users	Real-time accounting interval (minute)
1 to 99	3
100 to 499	6
500 to 999	12
≥1000	≥15

By default, *minute* is set to 12 minutes.

2.3.8 Setting Maximum Times of Real-time Accounting Request Failing to be Responded

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 for long, it will consider that there is device failure and stop accounting. Accordingly, it is necessary to disconnect the user at NAS end and on RADIUS server synchronously when some unpredictable failure exists. Quidway Series 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.

You can use the following command to set the maximum times of real-time accounting request failing to be responded

Perform the following configurations in RADIUS scheme view.

Table 2-19 Setting maximum times of real-time accounting request failing to be responded

Operation	Command
Set maximum times of real-time accounting request failing to be responded	**retry realtime-accounting** *retry-times*
Restore the maximum times to the default value	**undo retry realtime-accounting**

How to calculate the value of *retry-times*? Suppose that 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.

By default, the real-time accounting request can fail to be responded no more than 5 times.

2.3.9 Enabling/Disabling Stopping Accounting Request Buffer

Because the stopping accounting request concerns account balance and will affect the amount of charge, which is very important for both the subscribers and the ISP, NAS shall make its best effort to send the message to RADIUS accounting server. Accordingly, if the message from Quidway Series Switches to RADIUS accounting server has not been responded, switch shall save it in the local buffer and retransmit it until the server responds or discards the messages after transmitting for specified times. The following command can be used for setting to save the message or not. If save, use the command to set the maximum retransmission times.

Perform the following configurations in RADIUS scheme view.

Table 2-20 Enabling/Disabling stopping accounting request buffer

Operation	Command
Enable stopping accounting request buffer	**stop-accounting-buffer enable**
Disable stopping accounting request buffer	**undo stop-accounting-buffer enable**

By default, the stopping accounting request will be saved in the buffer.

2.3.10 Setting the Maximum Retransmitting Times of Stopping Accounting Request

Because the stopping accounting request concerns account balance and will affect the amount of charge, which is very important for both the subscribers and the ISP, NAS shall make its best effort to send the message to RADIUS accounting server. Accordingly, if the message from Quidway Series Switch to RADIUS accounting server has not been responded, switch shall save it in the local buffer and retransmit it until the server responds or discards the messages after transmitting for specified times. Use the command to set the maximum retransmission times.

Perform the following configurations in RADIUS scheme view.

Table 2-21 Setting the maximum retransmitting times of stopping accounting request

Operation	Command
Set the maximum retransmitting times of stopping accounting request	**retry stop-accounting** *retry-times*
Restore the maximum retransmitting times of stopping accounting request to the default value	**undo retry stop-accounting**

By default, the stopping accounting request can be retransmitted for up to 500 times.

2.3.11 Setting the Supported Type of RADIUS Server

Quidway Series Switches support the standard RADIUS protocol and the extended RADIUS service platforms, such as IP Hotel, 201+ and Portal, independently developed by Huawei.

You can use the following command to set the supported types of RADIUS servers.

Perform the following configurations in RADIUS scheme view.

Table 2-22 Setting the supported type of RADIUS server

Operation	Command
Setting the Supported Type of RADIUS Server	**server-type** { **huawei** | **iphotel** | **portal** | **standard** }
Restore the Supported Type of RADIUS Server to the default setting	**undo server-type**

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.

2.3.12 Setting RADIUS Server State

For the primary and second servers (no matter it is an authentication/authorization server or accounting server), if the primary 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. The following commands can be 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 both **active** or **block**, NAS will send the packets to the primary server only.

Perform the following configurations in RADIUS scheme view.

Table 2-23 Setting RADIUS server state

Operation	Command
Set the state of primary RADIUS server	**state primary** { **accounting** | **authentication** } { **block** | **active** }
Set the state of second RADIUS server	**state secondary**{ **accounting** | **authentication** } { **block** | **active** }

By default, the state of each server in RADIUS scheme is **active**.

2.3.13 Setting Username Format Transmitted to RADIUS Server

As mentioned above, the supplicants are generally named in userid@isp-name format. The part following "@" is the ISP domain name. Quidway Series Switches will put the users into different ISP domains according to the domain names. However, some earlier RADIUS servers reject the username including ISP domain name. In this case, you have to remove the domain name before sending the username to the RADIUS server. The following command of switch decides whether the username to be sent to RADIUS server carries ISP domain name or not.

Perform the following configurations in RADIUS scheme view.

Table 2-24 Setting username format transmitted to RADIUS server

Operation	Command
Set Username Format Transmitted to RADIUS Server	**user-name-format** { **with-domain** | **without-domain** }

Note:

If a RADIUS scheme is configured not to allow usernames including ISP domain names, the RADIUS scheme shall not be simultaneously used in more than one ISP domain. 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.)

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.

2.3.14 Setting the Unit of Data Flow that Transmitted to RADIUS Server

The following command defines the unit of the data flow sent to RADIUS server.

Perform the following configurations in RADIUS scheme view.

Table 2-25 Setting the unit of data flow transmitted to RADIUS server

Operation	Command
Set the unit of data flow transmitted to RADIUS server	**data-flow-format data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** }
Restore the unit to the default setting	**undo data-flow-format**

By default, the default data unit is byte and the default data packet unit is one packet.

2.3.15 Configuring Local RADIUS Authentication 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 authentication server function, i.e. realize basic RADIUS function on the switch.

Perform the following commands in system view to create/delete local RADIUS authentication server.

Table 2-26 Creating/Deleting local RADIUS authentication server

Operation	Command
Create local RADIUS authentication server	**local-server nas-ip** *ip-address* **key** *password*
Delete local RADIUS authentication server	**undo local-server nas-ip** *ip-address*

By default, the IP address of local RADIUS authentication server is 127.0.0.1 and the password is Huawei.

When using local RADIUS authentication server function, note that,

1) The number of UDP port used for authentication is 1645 and that for accounting is 1646.
2) The password configured by **local-server** command must be the same as that of the RADIUS authentication/authorization packet configured by the command **key authentication** in RADIUS scheme view.

2.4 Displaying and Debugging AAA and RADIUS Protocol

After the above configuration, execute **display** command in any view to display the running of the AAA and RADIUS configuration, and to verify the effect of the configuration. Execute **reset** command in user view to reset AAA and RADIUS statistics, etc. Execute **debugging** command in user view to debug AAA and RADIUS.

Table 2-27 Displaying and debugging AAA and RADIUS protocol

Operation	Command
Display the configuration information of the specified or all the ISP domains.	**display domain** [*isp-name*]
Display related information of user's connection	**display connection** [**access-type dot1x** | **domain** *isp-name* | **interface** *portnum* | **ip** *ip-address* | **mac** *mac-address* | **radius-scheme** *radius-scheme-name* | **vlan** *vlanid* | **ucibindex** *ucib-index* | **user-name** *user-name*]
Display related information of the local user	**display local-user** [**domain** *isp-name* | **idle-cut** { **disable** | **enable** } | **service-type** { **telnet** | **ftp** | **lan-access** | **ssh** } | **state** { **active** | **block** } | **user-name** *user-name* | **vlan** vlan-*id*]
Display the statistics of local RADIUS authentication server	**display local-server statistics**
Display the configuration information of all the RADIUS schemes or a specified one	**display radius** [*radius-scheme-name*]
Display the statistics of RADIUS packets	**display radius statistics**
Display the stopping accounting requests saved in buffer without response (from system view)	**display stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }
Delete the stopping accounting requests saved in buffer without response (from system view)	**reset stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }
Reset the statistics of RADIUS server.	**reset radius statistics**
Enable RADIUS packet debugging	**debugging radius packet**
Disable RADIUS packet debugging	**undo debugging radius packet**
Enable debugging of local RADIUS authentication server	**debugging local-server** { **all** | **error** | **event packet** }

Operation	Command
Disable debugging of local RADIUS authentication server	**undo debugging local-server** { **all** | **error** | **event packet** }

2.5 AAA and RADIUS Protocol Configuration Examples

For the hybrid configuration example of AAA/RADIUS protocol and 802.1x protocol, refer to Configuration Example in 802.1x Configuration. It will not be detailed here.

2.5.1 Configuring FTP/Telnet User Authentication at Remote RADIUS Server

Note:

Configuring Telnet user authentication at the remote server is similar to configuring FTP users. The following description is based on Telnet users.

I. Networking Requirements

In the environment as illustrated in the following figure, it is required to achieve through proper configuration that the RADIUS server authenticates the Telnet users to be registered.

One RADIUS server (as authentication server) is connected to the switch and the server IP address is 10.110.91.164. The password for exchanging messages between the switch and the authentication server is "expert". The switch cuts off domain name from username and sends the left part to the RADIUS server.

II. Networking Topology

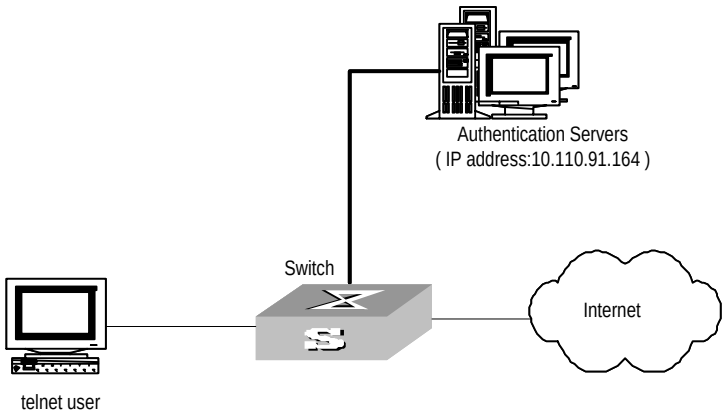


Figure 2-2 Configuring remote RADIUS authentication for Telnet users

III. Configurtion Schedule

Add a Telnet user.

Omitted

Note:

For details about configuring FTP and Telnet users, refer to User Interface Configuration in Getting Started.

Configure remote authentication mode for the Telnet user, i.e. scheme mode.

```
[Quidway-ui-vty0-4] authentication-mode scheme
```

Configure domain.

```
[Quidway] domain cams
[Quidway-isp-cams] quit
```

Configure RADIUS scheme.

```
[Quidway] radius scheme cams
[Quidway-radius-cams] primary authentication 10.110.91.164 1812
[Quidway-radius-cams] key authentication expert
[Quidway-radius-cams] server-type huawei
[Quidway-radius-cams] user-name-format without-domain
```

Configuration association between domain and RADIUS.

```
[Quidway-radius-cams] quit
[Quidway] domain cams
[Quidway-isp-cams] radius-scheme cams
```

2.5.2 Configuring FTP/Telnet User Authentication at Local RADIUS Server

Local RADIUS authentication of Telnet/FTP users is similar to remote RADIUS authentication. But you should modify the server IP address to 127.0.0.1, authentication password to Huawei, the UDP port number of the authentication server to 1645.

Note:

For details about local RADIUS authentication of Telnet/FTP users, refer to “2.3.15 Configuring Local RADIUS Authentication Server”.

2.5.3 Configuring Dynamic VLAN with RADIUS Server

I. Networking Requirements

The RADIUS server (taking Windows IAS as example) delivers sting VLAN ID “test”, which corresponds to the name of VLAN 100 on the switch. The switch can add the port to VLAN 100 when the server delivers "test".

II. Networking diagram

See Figure 2-2.

III. Configuration procedure

1) Specify RADIUS scheme

```
[Quidway] radius scheme ias
[Quidway-radius-ias] primary authentication 10.11.1.1
[Quidway-radius-ias] primary accounting 10.11.1.2
[Quidway-radius-ias] key authentication hello
[Quidway-radius-ias] key accounting hello
[Quidway-radius-ias] quit
```

2) Create ISP domain

```
[Quidway] domain ias
[Quidway-isp-ias] scheme radius-scheme ias
```

3) Configure VLAN delivery mode as string

```
[Quidway-isp-ias] vlan-assignment-mode string
[Quidway-isp-ias] quit
```

4) Create a VLAN and specify its name.

Create a VLAN.

```
[Quidway] vlan 100
```

Configure name of the delivered VLAN.

```
[Quidway-vlan100] name test
```

5) Configure on the Windows IAS server the VLAN delivery mode to string and the name of the delivered VLAN to “test”.

2.6 AAA and RADIUS Protocol Fault Diagnosis and Troubleshooting

RADIUS protocol of TCP/IP protocol suite is located on the application layer. It mainly specifies how to exchange user information between NAS and RADIUS server of ISP. So it is very likely to be invalid.

- Fault one: User authentication/authorization always fails

Troubleshooting:

1) The username may not be in the userid@isp-name format or NAS has not been configured with a default ISP domain. Please use the username in proper format and configure the default ISP domain on NAS.
2) The user may have not been configured in the RADIUS server database. Check the database and make sure that the configuration information of the user does exist in the database.
3) The user may have input a wrong password. So please make sure that the supplicant inputs the correct password.
4) The encryption keys of RADIUS server and NAS may be different. Please check carefully and make sure that they are identical.
5) There might be some communication fault between NAS and RADIUS server, which can be discovered through pinging RADIUS from NAS. So please ensure the normal communication between NAS and RADIUS.

- Fault two: RADIUS packet cannot be transmitted to RADIUS server.

Troubleshooting:

1) The communication lines (on physical layer or link layer) connecting NAS and RADIUS server may not work well. So please ensure the lines work well.
2) The IP address of the corresponding RADIUS server may not have been set on NAS. Please set a proper IP address for RADIUS server.
3) UDP ports of authentication/authorization and accounting services may not be set properly. So make sure they are consistent with the ports provided by RADIUS server.

- Fault three: After being authenticated and authorized, the user cannot send charging bill to the RADIUS server.

Troubleshooting:

1) The accounting port number may be set improperly. Please set a proper number.
2) The accounting service and authentication/authorization service are provided on different servers, but NAS requires the services to be provided on one server (by specifying the same IP address). So please make sure the settings of servers are consistent with the actual conditions.

Chapter 3 HABP Configuration

3.1 HABP Overview

If 802.1x attribute is configured at a switch, on a switch, 802.1x will run authentication at those ports where 802.1x is enabled. Only those which pass the authentication are able to forward packets. 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. HABP(Huawei Authentication Bypass Protocol) attribute can be used to solve this problem.

HABP packets contain the MAC address and other information of the member switches. When HABP attribute is enabled at the management switch, 802.1x authentication will be skipped for HABP packets, so management over switches is possible.

HABP includes HABP server and HABP client. In general, the server regularly sends HABP request packets to the client to collect the MAC addresses of the member switches, while the client responds to the request packets and forwards them to the lower-level switches. HABP server is often enabled at the management switch, while HABP client is at the member switches.

HABP attribute had better be enabled at a switch where 802.1x is enabled.

3.2 HABP configuration

HABP attribute configuration tasks include:

- Configuring HABP server
- Configuring HABP client

3.2.1 Configuring HABP Server

When HABP server is enabled, the management switch sends HABP request packets to its member switches to collect their MAC addresses, for the convenience of management. You can define the time interval for transmitting HABP request packets on the management switch.

To configure HABP server, follow these steps:

- Enable HABP attribute
- Configure HABP server
- Set time interval for HABP request transmission

Please perform the following operations in system view.

Table 3-1 Configuring HABP server

Operation	Command
Enable HABP attribute	**habp enable**
Restore HABP attribute to the default value	**undo habp enable**
Configure the switch as HABP Server	**habp server vlan** *vlan-id*
Delete HABP Server configuration	**undo habp server**
Set time interval for HABP request transmission	**habp timer** *interval*
Restore the time interval to the default value	**undo habp timer**

By default, HABP attribute is disabled at a switch, the HABP mode is client, and the time interval for HABP request transmission is 20 seconds.

3.2.2 Configuring HABP Client

HABP client runs at the member switches. Since the default HABP mode is client, you only need to enable HABP attribute at a switch.

Please perform the following operations in system view.

Table 3-2 Configuring HABP client

Operation	Command
Enable HABP attribute	**habp enable**
Restore HABP to the default value	**undo habp enable**

By default, HABP attribute is disabled at a switch.

3.3 Displaying and Debugging HABP Attribute

After the above configurations, you can view HABP attribute information using the **display** command in any view, or just for check. You can also debug HABP module using the **debugging** command in user view.

Table 3-3 Displaying and debugging HABP attribute

Operation	Command
Display configuration information and state of HABP attribute	**display habp**
Display MAC address table of HABP attribute	**display habp table**
Display HABP packet statistics	**display habp traffic**
Display HABP debugging state	**display debugging habp**

Operation	Command
Enable HABP debugging	**debugging habp**
Disable HABP debugging	**undo debugging habp**

HUAWEI

Quidway S3000-EI Series Ethernet Switches
Operation Manual

Network Protocol

Table of Contents

Chapter 1 ARP Configuration

1.1 Introduction to ARP

I. Necessity of ARP

An IP address cannot be directly used for communication between network devices because network devices can only identify MAC addresses. An IP address is only an address of a host in the network layer. To send the data packets transmitted through the network layer to the destination host, physical address of the host is required. So the IP address must be resolved into a physical address.

II. ARP implementation procedure

When two hosts on the Ethernet communicate, they must know the MAC addresses of each other. Every host will maintain the IP-MAC address translation table, which is known as ARP mapping table. A series of maps between IP addresses and MAC addresses of other hosts which were recently used to communicate with the local host are stored in the ARP mapping table. When a dynamic ARP mapping entry is not in use for a specified period of time, the host will remove it from the ARP mapping table so as to save the memory space and shorten the interval for switch to search ARP mapping table.

Suppose there are two hosts on the same network segment: Host A and Host B. The IP address of Host A is IP_A and the IP address of Host B is IP_B. Host A will transmit messages to Host B. Host A checks its own ARP mapping table first to make sure whether there are corresponding ARP entries of IP_B in the table. If the corresponding MAC address is detected, Host A will use the MAC address in the ARP mapping table to encapsulate the IP packet in frame and send it to Host B. If the corresponding MAC address is not detected, Host A will store the IP packet in the queue waiting for transmission, and broadcast it throughout the Ethernet. The ARP request packet contains the IP address of Host B and IP address and MAC address of Host A. Since the ARP request packet is broadcast, all hosts on the network segment can receive the request. However, only the requested host (i.e., Host B) needs to process the request. Host B will first store the IP address and the MAC address of the request sender (Host A) in the ARP request packet in its own ARP mapping table. Then Host B will generate an ARP reply packet into which, it will add MAC address of Host B, and then send it to Host A. The reply packet will be directly sent to Host A in stead of being broadcast. Receiving the reply packet, Host A will extract the IP address and the corresponding MAC address of Host B and add them to its own ARP mapping table. Then Host A will send Host B all the packets standing in the queue.

Normally, dynamic ARP executes and automatically searches for the resolution from the IP address to the Ethernet MAC address without the administrator.

1.2 Configure ARP

The ARP mapping table can be maintained dynamically or manually. Usually, the manually configured mapping from the IP addresses to the MAC addresses is known as static ARP. The user can display, add or delete the entries in the ARP mapping table through relevant manual maintenance commands.

The static ARP configuration includes:

- Manually Add/delete static ARP Mapping Entries
- Configure the dynamic ARP aging timer
- Enabling/Disabling ARP the Checking Function of ARP Entry

1.2.1 Manually Add/Delete Static ARP Mapping Entries

Perform the following configuration in System view.

Table 1-1 Manually add/delete static ARP mapping Entries

Operation	Command
Manually add a static ARP mapping entry	**arp static** *ip-address mac-address* [*vlan-id* { *interface-type interface-number* | *interface-name* }]
Manually delete a static ARP mapping entry	**undo arp** *ip-address*

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.

By default, the ARP mapping table is empty and the address mapping is obtained through dynamic ARP.

1.2.2 Configure the Dynamic ARP Aging Timer

For purpose of flexible configuration, the system provides the following commands to assign dynamic ARP aging period. When the system learns a dynamic ARP entry, its aging period is based on the current value configured.

Perform the following configuration in system view.

Table 1-2 Configure the dynamic ARP aging timer

Operation	Command
Configure the dynamic ARP aging timer	**arp timer aging** *aging-time*
restore the default dynamic ARP aging time	**undo arp timer aging**

By default, the aging time of dynamic ARP aging timer is 20 minutes.

1.2.3 Enabling/Disabling ARP the Checking Function of ARP Entry

You can use the following command to control the device whether to learn the ARP entry where the MAC address is multicast MAC address.

Perform the following configuration in system view.

Table 1-3 Enabling/Disabling ARP the checking function of ARP entry

Operation	Command
Enable the checking of ARP entry, that is, the device does not learn the ARP entry where the MAC address is multicast MAC address	**arp check enable**
Disable the checking of ARP entry, that is, the device learns the ARP entry where the MAC address is multicast MAC address	**undo arp check enable**

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.

1.3 Gratuitous ARP Configuration

1.3.1 Gratuitous ARP Overview

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 that of 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. For example, when a device receives a gratuitous ARP request existing in the cache of the device from an IP address, then the sending hardware address (such as Ethernet address) in the gratuitous ARP request needs to update the content in the cache. The above operation must be done when a device receives any gratuitous ARP request. ARP request is broadcast on the

network, so all hosts on the network must do this every time the ARP request is sent.

Characteristics of gratuitous ARP packets:

- The source and destination IP addresses are all native addresses, and the source MAC address of the packet is native MAC address.
- If another device receives a gratuitous ARP packet and finds out that the IP address in the ARP packet conflicts with that of its own, it sends an ARP reply back to the device sending the ARP packet.

1.3.2 Configuration Tasks

The configuration tasks of the gratuitous ARP are described in the following table:

Table 1-4 Configure gratuitous ARP

Sequence number	Configuration item	Command	Description
1	Enter system view	<Quidway> **system-view**	—
2	Enable ARP packet learning	[Quidway] **gratuitous-arp-learning enable**	Required

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

1.3.3 Configuration Example

I. Network requirements

Enable gratuitous ARP packet learning on the switch Quidway A.

II. Configuration procedure

```
<QuidwayA> system-view
[QuidwayA] gratuitous-arp-learning enable
```

1.4 Display and debug ARP

After the above configuration, execute **display** command in any view to display the running of the ARP configuration, and to verify the effect of the configuration. Execute **debugging** command in user view to debug ARP configuration. Execute **reset** command in user view to clear ARP mapping table.

Table 1-5 Display and debug ARP

Operation	Command
Display ARP mapping table	**display arp** [**static** | **dynamic** | *ip-address*]
Display the current setting of the dynamic ARP map aging timer	**display arp timer aging**
Reset ARP mapping table	**reset arp** [**dynamic** | **static** | **interface** { *interface-type interface-number* | *interface-name* }]
Enable ARP information debugging	**debugging arp packet**
Disable ARP information debugging	**undo debugging arp packet**

Chapter 2 DHCP-Snooping Configuration

2.1 DHCP-Snooping Overview

For security, the IP addresses used by online users may be recorded to confirm the association between the users' IP addresses and their MAC addresses. The Layer 3 Ethernet switch records the IP addresses obtained by the clients with DHCP Relay, while the Layer 2 Ethernet switch listens to the DHCP broadcast packets for this purpose.

To assign IP addresses to the clients, DHCP server transmits DHCPACK packets. After received the packets, the client can obtain an IP address. Snooping DHCPACK is a way to know the clients' IP addresses.

The client broadcasts DHCPREQUEST packet to request DHCP server to assign address. The IP address requested through DHCPREQUEST is the same as that assigned through DHCPACK. So snooping DHCPREQUEST is another way to know clients' IP addresses.

With DHCP-Snooping enabled, the switch can distract IP address and MAC address from the DHCPACK or DHCPREQUEST packets received and record them.

In addition, pseudo-DHCP servers in the network may cause users to get incorrect IP addresses. To guarantee that users can obtain IP address from the legal DHCP servers, DHCP-Snooping allows ports to be set as trusted or distrusted. The former ports connect DHCP servers or other switches and the latter ports connect users or network. Distrusted ports discard the DHCPACK and DHCPOFF packets from DHCP servers, whereas trusted ports forward these types of packets. In this way, users can get correct IP address.

2.2 Configure DHCP-Snooping

DHCP-Snooping configuration includes:

- Enable/Disable the DHCP-Snooping function of the Switch
- Setting the port as trusted port

2.2.1 Enable/Disable the DHCP-Snooping Function of the Switch

Perform the following configuration in System view.

Table 2-1 Enable/Disable the DHCP-Snooping function of the switch

Operation	Command
Enable the DHCP-Snooping function of the switch	**dhcp-snooping**
Disable the DHCP-Snooping function of the switch	**undo dhcp-snooping**

By default, the switch does not enable DHCP-Snooping function.

2.2.2 Setting the Port as Trusted Port

Perform the following configuration in Ethernet port view.

Table 2-2 Setting the port as trusted port

Operation	Command
Set the port as trusted port	**dhcp-snooping trust**
Restore the port as distrusted port	**undo dhcp-snooping trust**

By default, the ports of a switch are distrusted port.

2.3 Display and debug DHCP-Snooping

After the above configuration, execute **display** command in any view to display the clients' IP address and MAC address bindings recorded through DHCP-Snooping.

Table 2-3 Display and debug DHCP-Snooping

Operation	Command
Display the information of the DHCP-Snooping correspondence table	**display dhcp-snooping** [**vlan** { *vlan_list* | **all** }]
Display the number of the DHCP-Snooping entries in the binding table	**display dhcp-snooping count**
Display the status of DHCP-Snooping function and the information of trusted ports	**display dhcp-snooping trust**

Chapter 3 DHCP Client Configuration

3.1 Overview of DHCP Client

With expansion of network size and complication of network structure, network configuration becomes more and more complex. It is often the case that computers change physical positions frequently (portable computers and wireless networks for example) and that computers exceed the IP addresses available. Dynamic host configuration protocol (DHCP) has been developed right for this situation. DHCP is in client/server structure, with DHCP client dynamic requesting configuration information, while DHCP server returning configuration information base on the specific policies.

A typical DHCP application often contains a DHCP server and several clients (desktop and laptop PCs). See the following figure.

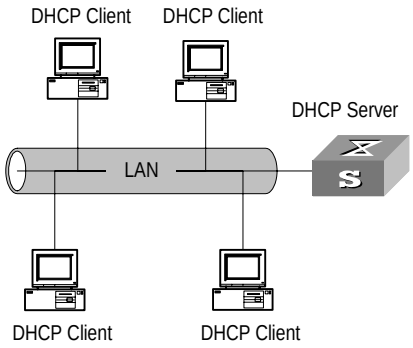


Figure 3-1 Typical DHCP application

To obtain valid dynamic IP addresses, DHCP client exchanges different types of information with the server at different stages. One of the following three situations may occur:

1) DHCP client logs into the network for the first time

When DHCP client logs into the network for the first time, its communication with the DHCP server includes these four stages:

- Discover stage, the stage when the DHCP client looks for the DHCP server. The client broadcasts the DHCP_Discover message and only the DHCP server can respond.
- Offer stage, the stage when the DHCP server allocates the IP address. After receiving the DHCP_Discover message from the client, the DHCP server chooses an IP address still available in IP address pool for the client, and sends to the client the DHCP_Offer message containing the leased IP address and other settings.
- Select stage, the stage when the client selects the IP address. If several DHCP servers send DHCP_Offer messages to the client, the client only accepts the first

received one and then broadcasts DHCP_Request messages respectively to those DHCP servers. The message contains the information of IP address request from the selected DHCP server.

- Acknowledge stage, the stage when the DHCP server acknowledges the IP address. When receiving the DHCP_Request message from the client, the DHCP server sends the DHCP_ACK message containing the allocated IP address and other settings back to the client. Then the DHCP client binds its TCP/IP components to the NIC (network interface card).

Other DHCP servers not selected still can allocate their IP addresses to other clients later.

2) DHCP client logs into the network for a second time

When DHCP client logs into the network for a second time, its communication with the DHCP server includes these stages:

- When the DHCP client logs into the network at the first time, then at later login the client only needs to broadcast the DHCP_Request message containing the IP address obtained last time, other than the DHCP_Dsicover message.
- After the reception of the DHCP_Request message, the DHCP server returns the DHCP_ACK message if the requested IP address is still not allocated, to indicate the client to continue use of the IP address.
- If the requested IP address becomes unavailable (for example, having been allocated to another client), the DHCP server returns the DHCP_NAK message. After receiving the DHCP_NAK message, the client sends the DHCP_Discover message to request another new IP address.

3) DHCP client extends its IP lease period

There is time limit for the IP addresses leased to DHCP clients. The DHCP server shall withdraw the IP addresses when their lease period expires. If the DHCP client wants to continue use of the old IP address, it has to extend the IP lease.

In practice, the DHCP client, by default, shall originate the DHCP_Request message to the DHCP server right in the middle of the IP lease period, to update the IP lease. If the IP address is still available, the DHCP server responds with the DHCP_ACK message, notifying the client that it has got the new IP lease.

The DHCP client implemented on the switch supports automatic IP lease update.

3.2 DHCP Client Configuration

DHCP client configuration include:

Configuring a VLAN interface to obtain IP address using DHCP

3.2.1 Configuring a VLAN Interface to Obtain IP Address Using DHCP

Perform the following configuration in VLAN interface view.

Table 3-1 Configuring a VLAN interface to obtain IP address using DHCP

Operation	Command
Configure VLAN interface to obtain IP address using DHCP	**ip address dhcp-alloc**
Remove the configuration	**undo ip address dhcp-alloc**

By default, the VLAN interface does not obtain IP address using DHCP.

3.3 Displaying and Debugging DHCP Client Configuration

After the above configuration, execute **display** command in any view to display the running of the DHCP Client configuration, and to verify the effect of the configuration. Execute **debugging** command in user view to debug DHCP Client configuration.

Table 3-2 Displaying and debugging DHCP Client configuration

Operation	Command
Display address allocation information of DHCP client	**display dhcp client** [**verbose**]
Enable/disable DHCP client debugging	[**undo**] **debugging dhcp client** { **all** | **error** | **event** | **packet** }

Chapter 4 BOOTP Client Configuration

4.1 Overview of BOOTP Client

BOOTP client can request the server to allocate an IP address to it using BOOTP (bootstrap protocol). These two major processes are included on the BOOTP client:

- Sending BOOTP Request message to the server
- Processing BOOTP Response message returned from the server

In obtaining IP address using BOOTP, BOOTP client sends the server the BOOTP Request message. Upon receiving the request message, the server returns the BOOTP Response message. BOOTP client then can obtain the allocated IP address from the received response message.

The BOOTP message is based on UDP, so retransmission mechanism in the event of timeout is used to guarantee its reliable transmission. BOOTP client also starts a retransmission timer when it sends the request message to the server. If the timer expires before the return of the response message from the server, the request message will be retransmitted. The retransmission occurs every five seconds and the maximum number of retransmission is 3, that is, the message shall not be retransmitted after the third time.

4.2 BOOTP Client Configuration

BOOTP client configuration includes:

Configuring a VLAN interface to obtain the IP address using BOOTP

4.2.1 Configuring a VLAN Interface to Obtain the IP Address Using BOOTP

Perform the following configuration in VLAN interface view.

Table 4-1 Configuring a VLAN interface to obtain the IP address using BOOTP

Operation	Command
Configure VLAN interface to obtain IP address using BOOTP	**ip address bootp-alloc**
Remove the configuration	**undo ip address bootp-alloc**

By default, the VLAN interface cannot use BOOTP to get IP address.

4.3 Displaying and Debugging BOOTP Client

After the above configuration, execute **display** command in any view to display the running of the BOOTP client configuration, and to verify the effect of the configuration.

Execute **debugging** command in user view to debug BOOTP client.

Table 4-2 Displaying and debugging BOOTP client

Operation	Command
Display information of BOOTP client	**display bootp client** [**interface vlan-interface** *vlan_id*]
Disable/enable BOOTP client debugging	[**undo**] **debugging bootp client**

Chapter 5 Access Management Configuration

5.1 Access Management Overview

One of the typical Ethernet access networking scenario is that the users access external network through the Ethernet switches. In this case, the external network is connected to the Ethernet switch. The Ethernet switch connects to the Hubs, each of which centralizes several PCs. The following figure illustrates the networking scenario.

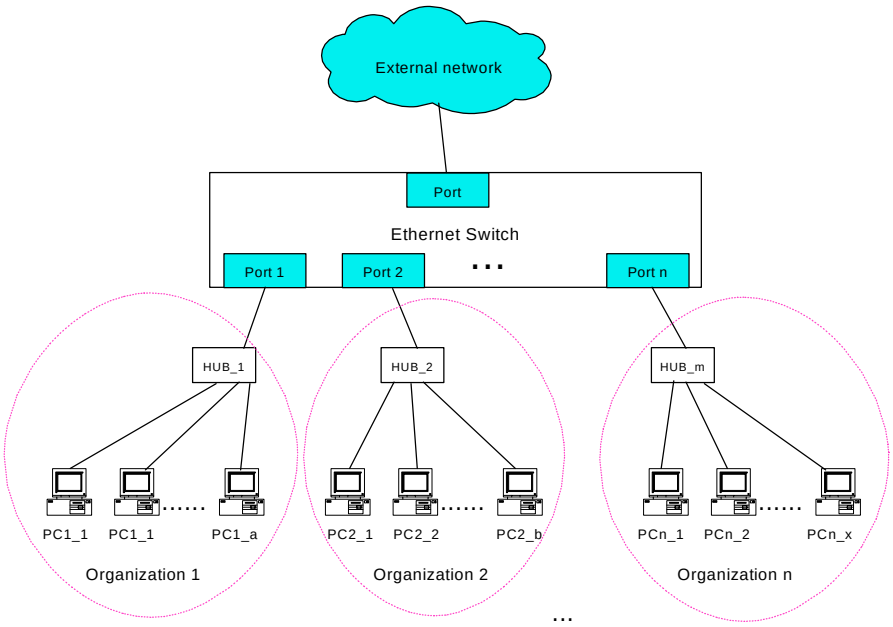


Figure 5-1 Typical Ethernet access networking scenario

If not-so-many users are connected to the switch, the ports allocated to different enterprises need to belong to the same VLAN and different enterprises should be isolated in the light of cost and security. All these requirements can be achieved with the access management function by the Ethernet switches. See Figure 5-1.

Isolation measure is required, because otherwise the PCs in two organizations may interwork with each other. The L2 isolation function at the switch port can ensure two ports do not receive the packets from the other port, so that only those PCs in the same organization can communicate with each other

5.2 Configure Access Management

Access management configuration includes:

- Enable access management function
- Configure Layer 2 isolation between ports

- Configure port, IP address and MAC address binding

5.2.1 Enable Access Management Function

You can use the following command to enable access management function. Only after the access management function is enabled will the access management features (IP and port binding and Layer 2 port isolation) take effect.

Perform the following configuration in System view.

Table 5-1 Enable/Disable access management function

Operation	Command
Enable access management function	**am enable**
Disable access management function	**undo am enable**

By default, the system disables the access management function.

5.2.2 Configure Layer 2 Isolation between Ports

You can use the following command to set 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 ports (group).

Perform the following configuration in Ethernet interface view.

Table 5-2 Configure Layer 2 isolation between ports

Operation	Command
Configure Layer 2 isolation between ports	**am isolate** *interface-list*
Cancel Layer 2 isolation between ports	**undo am isolate** *interface-list*

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.

5.2.3 Configure Port, IP Address and MAC Address Binding

Perform the following actions to bind the port, IP address and MAC address.

The system supports the following binding combination: Port+IP, Port+MAC, Port+IP+MAC, and IP+MAC.

- Port+IP binding: binding the packet's receiving port and its source IP address. The specified port will only allow the packet with specified IP address to pass; meanwhile the packet with specified IP address can only pass through the specified port.

- Port+MAC binding: binding the packet's receiving port and its source MAC address. The specified port will only allow the packet with specified MAC address to pass; meanwhile the packet with specified MAC address can only pass through the specified port.
- Port+IP+MAC binding: binding the packet's receiving port, source IP address and source MAC address. The specified port will only allow the packet with specified IP and MAC address to pass. The packet with specified IP address can only pass through the specified port. Likewise, the packet with specified MAC address can only pass from the specified port.
- IP+MAC binding: binding the packet's source IP address and its source MAC address. If the packet's source IP address and its specified IP is the same, then the packet is relayed only when its source MAC address is the specified MAC address. Likewise, if the packet's source MAC is the same as the specified MAC address, then the packet is relayed only when its source IP address is the same as the specified IP address.

Perform the following configuration in the system view.

Table 5-3 Binding Port, IP Address and MAC Address

Operation	Command
Bind port, IP address and MAC address	**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* }* }
Remove the binding of port, IP address and MAC address binding	**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* }* }

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.

5.3 Display and debug Access Management

After the above configuration, execute **display** command in any view to display the current configurations of access management on the ports, and to verify the effect of the configuration.

Table 5-4 Display current configuration of access management

Operation	Command
Display current configuration of access management	**display am** [*interface-list*]
Display Port, IP address and MAC address binding	**display am user-bind** [**interface** { *interface-name* | *interface-type interface-number* } | **mac-addr** *mac* | **ip-addr** *ip*]

5.4 Access Management Configuration Example

I. Networking requirements

Organization 1 is connected to the port 1 of the switch, and organization 2 to the port 2.The ports 1 and 2 belong to the same VLAN. Organization 1 and organization 2 cannot communicate with each other.

II. Networking diagram

See Figure 5-1.

III. Configuration procedure

Enable access management globally.

```
[Quidway] am enable
```

Configures Layer 2 isolation between port 1 and port 2.

```
[Quidway-Ethernet0/1] am isolate ethernet0/2
```

Chapter 6 IP Performance Configuration

6.1 IP Performance Configuration

IP performance configuration includes:

Configure TCP attributes

6.1.1 Configure TCP Attributes

TCP attributes that can be configured include:

- synwait timer: When sending the syn packets, TCP starts the synwait timer. If response packets are not received before synwait timeout, the TCP connection will be terminated. The timeout of synwait timer ranges 2 to 600 seconds and it is 75 seconds by default.
- finwait timer: When the TCP connection state turns from FIN_WAIT_1 to FIN_WAIT_2, finwait timer will be started. If FIN packets are not received before finwait timer timeout, the TCP connection will be terminated. Finwait timer ranges 76 to 3600 seconds. By default, finwait timer is 675 seconds.
- The receiving/sending buffer size of connection-oriented Socket is in the range from 1 to 32K bytes and is 8K bytes by default.

Perform the following configuration in System view.

Table 6-1 Configure TCP attributes

Operation	Command
Configure synwait timer time for TCP connection establishment	**tcp timer syn-timeout** *time-value*
Restore synwait timer time for TCP connection establishment to default value	**undo tcp timer syn-timeout**
Configure FIN_WAIT_2 timer time of TCP	**tcp timer fin-timeout** *time-value*
Restore FIN_WAIT_2 timer time of TCP to default value	**undo tcp timer fin-timeout**
Configure the Socket receiving/sending buffer size of TCP	**tcp window** *window-size*
Restore the socket receiving/sending buffer size of TCP to default value	**undo tcp window**

By default, the TCP finwait timer is 675 seconds, the synwait timer is 75 seconds, and the receiving/sending buffer size of connection-oriented Socket is 8K bytes.

6.2 Display and debug IP Performance

After the above configuration, execute **display** command in any view to display the running of the IP Performance configuration, and to verify the effect of the configuration. Execute **reset** command in user view to clear IP and TCP statistics information.

Table 6-2 Display and debug IP performance

Operation	Command
Display TCP connection state	**display tcp status**
Display TCP connection statistics data	**display tcp statistics**
Display IP statistics information	**display ip statistics**
Display ICMP statistics information	**display icmp statistics**
Display socket interface information of current system	**display ip socket** [**socktype** *sock-type*] [**task-id** *socket-id*]
Display the summary of the Forwarding Information Base	**display fib**
Reset IP statistics information	**reset ip statistics**
Reset TCP statistics information	**reset tcp statistics**

6.3 Troubleshoot IP Performance

Fault: IP layer protocol works normally but TCP and UDP cannot work normally.

In the event of such a fault, you can enable the corresponding debugging information output to view the debugging information.

- Use the **terminal debugging** command to output the debugging information to the console.
- Use the command **debugging udp packet** to enable the UDP debugging to trace the UDP packet.

The following are the UDP packet formats:

```
UDP output packet:
Source IP address:202.38.160.1
Source port:1024
Destination IP Address 202.38.160.1
Destination port: 4296
```

- Use the **debugging tcp packet** command to enable the TCP debugging to trace the TCP packets.

Operations include:

```
[Quidway] terminal debugging
```

```
<Quidway> debugging tcp packet
```

Then the TCP packets received or sent can be checked in real time. Specific packet formats include:

```
TCP output packet:
Source IP address:202.38.160.1
Source port:1024
Destination IP Address 202.38.160.1
Destination port: 4296
Sequence number :4185089
Ack number: 0
Flag  :SYN
Packet length :60
Data offset: 10
```

HUAWEI

Quidway S3000-EI Series Ethernet Switches
Operation Manual

System Management

Table of Contents

Chapter 1 File System Management

1.1 File System

1.1.1 File System Overview

The Ethernet switch provides a file system module for user's efficient management over the storage devices such as flash memory. The file system offers file access and directory management, mainly including creating the file system, creating, deleting, modifying and renaming a file or a directory and opening a file.

By default, the file system needs user's confirmation before executing the commands, such as deleting or overwriting a file, which may make losses.

Based on the operated objects, the file system can be divided as follows:

- Directory operation
- File operation
- Storage device operation
- Set the prompt mode of the file system

1.1.2 Directory Operation

The file system can be used to create or delete a directory, display the current working directory, and display the information about the files or directories under a specified directory. You can use the following commands to perform directory operations.

Perform the following configuration in user view.

Table 1-1 Directory operation

Operation	Command
Create a directory	**mkdir** *directory*
Delete a directory	**rmdir** *directory*
Display the current working directory	**pwd**
Display the information about directories or files	**dir** [/ **all**] [*file-url*]
Change the current directory	**cd** *directory*

1.1.3 File Operation

The file system can be used to delete or undelete a file and permanently delete a file. Also, it can be used to display file contents, rename, copy and move a file and display

the information about a specified file. You can use the following commands to perform file operations.

Perform the following configuration in user view.

Table 1-2 File operation

Operation	Command
Delete a file	**delete** [/**unreserved**] *file-url*
Undelete a file	**undelete** *file-url*
Delete a file from the recycle bin permanently	**reset recycle-bin** *file-url*
View contents of a file	**more** *file-url*
Rename a file	**rename** *fileurl-source fileurl-dest*
Copy a file	**copy** *fileurl-source fileurl-dest*
Move a file	**move** *fileurl-source fileurl-dest*
Display the information about directories or files	**dir** [/ **all**] [*file-url*]

1.1.4 Storage Device Operation

The file system can be used to format a specified memory device. You can use the following commands to format a specified memory device.

Perform the following configuration in user view.

Table 1-3 Storage device operation

Operation	Command
Format the storage device	**format** *filesystem*

1.1.5 Set the Prompt Mode of the File System

The following command can be used for setting the prompt mode of the current file system.

Perform the following configuration in system view.

Table 1-4 File system operation

Operation	Command
Set the file system prompt mode.	**file prompt** { **alert** | **quiet** }

1.2 Configure File Management

1.2.1 Configure File Management Overview

The management module of configuration file provides a user-friendly operation interface. It saves the configuration of the Ethernet switch in the text format of command line to record the whole configuration process. Thus you can view the configuration information conveniently.

The format of configuration file includes:

- It is saved in the command format.
- Only the non-default constants will be saved
- The organization of commands is based on command views. The commands in the same command mode are sorted in one section. The sections are separated with a blank line or a comment line (A comment line begins with exclamation mark "#").
- Generally, the sections in the file are arranged in the following order: system configuration, ethernet port configuration, vlan interface configuration, routing protocol configuration and so on.
- It ends with "end".

The management over the configuration files includes:

- Display the Current-configuration and Saved-configuration of Ethernet Switch
- Save the Current-configuration
- Erase configuration files from Flash Memory

1.2.2 Display the Current-configuration and Saved-configuration of Ethernet Switch

After being powered on, the system will read the configuration files from Flash for the initialization of the device. (Such configuration files are called saved-configuration files). If there is no configuration file in Flash, the system will begin the initialization with the default parameters. Relative to the saved-configuration, the configuration in effect during the operating process of the system is called current-configuration. You can use the following commands to display the current-configuration and saved-configuration information of the Ethernet switch.

Perform the following configuration in any view.

Table 1-5 Display the configurations of the Ethernet switch

Operation	Command
Display the saved-configuration information of the Ethernet switch	**display saved-configuration**
Display the current-configuration information of the Ethernet switch	**display current-configuration** [**controller** | **interface** *interface-type* [*interface-number*] | **configuration** [**post-system | system** | **user-interface**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Note:

The configuration files are displayed in their corresponding saving formats.

1.2.3 Save the Current-configuration

Use the **save** command to save the current-configuration in the Flash Memory, and the configurations will become the saved-configuration when the system is powered on for the next time.

Perform the following configuration in user view.

Table 1-6 Save the current-configuration

Operation	Command
Save the current-configuration	**save**

1.2.4 Erase Configuration Files from Flash Memory

The **reset saved-configuration** command can be used to erase configuration files from Flash Memory. The system will use the default configuration parameters for initialization when the Ethernet switch is powered on for the next time.

Perform the following configuration in user view.

Table 1-7 Erase configuration files from Flash Memory

Operation	Command
Erase configuration files from Flash Memory	**reset saved-configuration**

You may erase the configuration files from the Flash in the following cases:

- After being upgraded, the software does not match with the configuration files.

- The configuration files in flash are damaged. (A common case is that a wrong configuration file has been downloaded.)

1.3 FTP

1.3.1 FTP Overview

FTP is a common way to transmit files on the Internet and IP network. Before the World Wide Web (WWW), files were transmitted in the command line mode and FTP was the most popular application. Even now, FTP is still used widely, while most users transmit files via Email and Web.

FTP, a TCP/IP protocol on the application layer, is used for transmitting files between a remote server and a local host.

The Ethernet switch provides the following FTP services:

- FTP server: You can run FTP client program to log in the server and access the files on it.
- FTP client: After connected to the server through running the terminal emulator or Telnet on a PC, you can access the files on it, using FTP command.

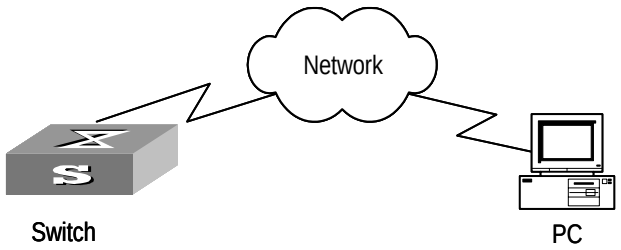


Figure 1-1 FTP configuration

Table 1-8 Configuration of the switch as FTP client

Device	Configuration	Default	Description
Switch	Log into the remote FTP server directly with the **ftp** command.	--	You need first get FTP user command and password, and then log into the remote FTP server. Then you can get the directory and file authority.
PC	Start FTP server and make such settings as username, password, authority.	--	--

Table 1-9 Configuration of the switch as FTP server

Device	Configuration	Default	Description
Switch	Start FTP server.	FTP server is disabled.	You can view the configuration information of FTP server with the **ftp-server** command.
	Configure authentication and authorization for FTP server.	--	Configure username, password and authorized directory for FTP users.
	Configure running parameters for FTP server.		Configure timeout time value for FTP server.
PC	Log into the switch from FTP client.	--	--

Caution:

The prerequisite for normal FTP function is that the switch and PC are reachable.

1.3.2 Enable/Disable FTP Server

You can use the following commands to enable/disable the FTP server on the switch. Perform the following configuration in system view.

Table 1-10 Enable/Disable FTP Server

Operation	Command
Enable the FTP server	**ftp server enable**
Disable the FTP server	**undo ftp server**

FTP server supports multiple users to access at the same time. A remote FTP client sends request to the FTP server. Then, the FTP server will carry out the corresponding operation and return the result to the client.

By default, FTP server is disabled.

1.3.3 Configure the FTP Server Authentication and Authorization

You can use the following commands to configure FTP server authentication and authorization. The authorization information of FTP server includes the top working directory provided for FTP clients.

Perform the following configuration in corresponding view.

Table 1-11 Configure the FTP Server Authentication and Authorization

Operation	Command
Create new local user and enter local user view(system view)	**local-user** *username*
Delete local user(system view)	**undo local-user** [*username* | **all** [**service-type ftp**]]
Configure password for local user(local user view)	**password** [**cipher** | **simple**] *password*
Configure service type for local user(local user view)	**service-type ftp ftp-directory** *directory*
Cancel password for local user(local user view)	**undo password**
Cancel service type for local user(local user view)	**undo service-type ftp** [**ftp-directory**]

Only the clients who have passed the authentication and authorization successfully can access the FTP server.

1.3.4 Configure the Running Parameters of FTP Server

You can use the following commands to configure the connection timeout of the FTP server. If the FTP server receives no service request from the FTP client for a period of time, it will cut the connection to it, thereby avoiding the illegal access from the unauthorized users. The period of time is FTP connection timeout.

Perform the following configuration in system view.

Table 1-12 Configure FTP server connection timeout

Operation	Command
Configure FTP server connection timeouts	**ftp timeout** *minute*
Restoring the default FTP server connection timeouts	**undo ftp timeout**

By default, the FTP server connection timeout is 30 minutes.

1.3.5 Display and Debug FTP Server

After the above configuration, execute **display** command in any view to display the running of the FTP Server configuration, and to verify the effect of the configuration.

Table 1-13 Display and debug FTP Server

Operation	Command
Display FTP server	**display ftp-server**
Display the connected FTP users.	**display ftp-user**

The **display ftp-server** command can be used for displaying the configuration information about the current FTP server, including the maximum amount of users supported by FTP server and the FTP connection timeout. The **display ftp-user** command can be used for displaying the detail information about the connected FTP users.

1.3.6 Introduction to FTP Client

As an additional function provided by Ethernet switch, FTP client is an application module and has no configuration functions. The switch connects the FTP clients and the remote server and inputs the command from the clients for corresponding operations (such as creating or deleting a directory).

1.3.7 FTP client configuration example

I. Networking requirement

The switch serves as FTP client and the remote PC as FTP server. The configuration on FTP server: Configure a FTP user named as switch, with password hello and with read & write authority over the Switch root directory on the PC. The IP address of a VLAN interface on the switch is 1.1.1.1, and that of the PC is 2.2.2.2. The switch and PC are reachable.

The switch application switch.app is stored on the PC. Using FTP, the switch can download the switch.app from the remote FTP server and upload the vrpcfg.txt to the FTP server under the switch directory for backup purpose.

II. Networking diagram

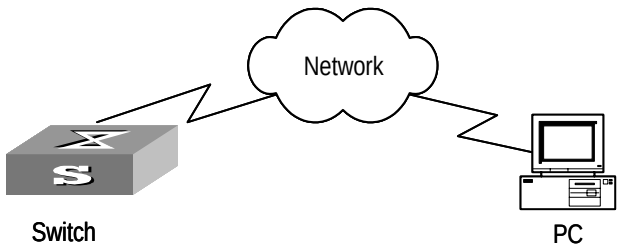


Figure 1-2 Networking for FTP configuration

III. Configuration procedure

1) Configure FTP server parameters on the PC: a user named as switch, password hello, read & write authority over the Switch directory on the PC.
2) Configure the switch

Log into the switch (locally through the Console port or remotely using Telnet).

```
<Quidway>
```

Caution:

If the flash memory of the switch is not enough, you need to first delete the existing programs in the flash memory and then upload the new ones.

Type in the right command in user view to establish FTP connection, then correct username and password to log into the FTP server.

```
<Quidway> ftp 2.2.2.2
Trying ...
Press CTRL+K to abort
Connected.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(none):switch
331 Give me your password, please
Password:*****
230 Logged in successfully
[ftp]
```

Type in the authorized directory of the FTP server.

```
[ftp] cd switch
```

Use the **put** command to upload the vrpcfg.txt to the FTP server.

```
[ftp] put vrpcfg.txt
```

Use the **get** command to download the switch.app from the FTP server to the flash directory on the FTP server.

```
[ftp] get switch.app
```

Use the **quit** command to release FTP connection and return to user view.

```
[ftp] quit
<Quidway>
```

Use the **boot boot-loader** command to specify the downloaded program as the application at the next login and reboot the switch.

```
<Quidway> boot boot-loader switch.app
<Quidway> reboot
```

1.3.8 FTP server configuration example

I. Networking requirement

Switch serves as FTP server and the remote PC as FTP client. The configuration on FTP server: Configure a FTP user named as switch, with password hello and with read & write authority over the flash root directory on the PC. The IP address of a VLAN interface on the switch is 1.1.1.1, and that of the PC is 2.2.2.2. The switch and PC are reachable.

The switch application switch.app is stored on the PC. Using FTP, the PC can upload the switch.app from the remote FTP server and download the vrpcfg.txt from the FTP server for backup purpose.

II. Networking diagram

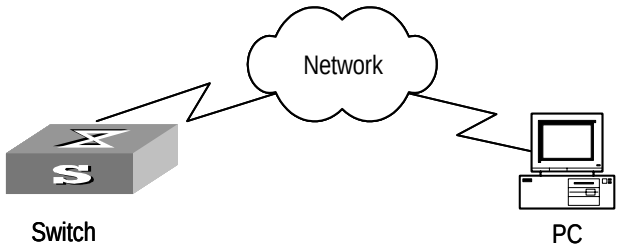


Figure 1-3 Networking for FTP configuration

1) Configure the switch

Log into the switch (locally through the Console port or remotely using Telnet).

```
<Quidway>
```

Start FTP function and set username, password and file directory.

```
[Quidway] ftp server enable
[Quidway] local-user switch
[Quidway-luser-switch] service-type ftp ftp-directory flash:
[Quidway-luser-switch] password simple hello
```

2) Run FTP client on the PC and establish FTP connection. Upload the switch.app to the switch under the Flash directory and download the vrpcfg.txt from the switch. FTP client is not shipped with the switch, so you need to buy it separately.

Caution:

If the flash memory of the switch is not enough, you need to first delete the existing programs in the flash memory and then upload the new ones.

3) When the uploading is completed, initiate file upgrade on the switch.

```
<Quidway>
```

Use the **boot boot-loader** command to specify the downloaded program as the application at the next login and reboot the switch.

```
<Quidway> boot boot-loader switch.app
<Quidway> reboot
```

1.4 TFTP

1.4.1 TFTP Overview

Trivial File Transfer Protocol (TFTP) is a simple protocol for file transmission. Compared with FTP, another file transmission protocol, TFTP has no complicated interactive access interface or authentication control, and therefore it can be used when there is no complicated interaction between the clients and server. TFTP is implemented on the basis of UDP.

TFTP transmission is originated from the client end. To download a file, the client sends a request to the TFTP server and then receives data from it and sends acknowledgement to it. To upload a file, the client sends a request to the TFTP server and then transmits data to it and receives the acknowledgement from it. TFTP transmits files in two modes, binary mode for program files and ASCII mode for text files.

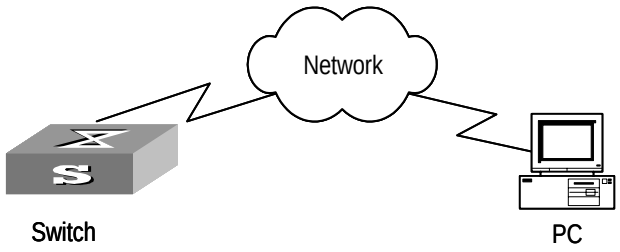


Figure 1-4 TFTP configuration

Table 1-14 Configuration of the switch as TFTP client

Device	Configuration	Default	Description
Switch	Configure IP address for the VLAN interface of the switch, in the same network segment as that of TFTP server.	--	TFTP is right for the case where no complicated interactions are required between the client and server. Make sure that the IP address of the VLAN interface on the switch is in the same network segment as that of the TFTP server.
	Use the **tftp** command to log into the remote TFTP server for file uploading and downloading.	-	-
PC	Start TFTP server and set authorized TFTP directory.	-	--

1.4.2 Configure the File Transmission Mode

TFTP transmits files in two modes, binary mode for program files and ASCII mode for text files. You can use the following commands to configure the file transmission mode.

Perform the following configuration in system view.

Table 1-15 Configure the file transmission mode

Operation	Command
Configure the file transmission mode	**tftp** { **ascii	binary** }

By default, TFTP transmits files in binary mode.

1.4.3 Download Files by means of TFTP

To download a file, the client sends a request to the TFTP server and then receives data from it and sends acknowledgement to it. You can use the following commands to download files by means of TFTP.

Perform the following configuration in system view.

Table 1-16 Download files by means of TFTP

Operation	Command
Download files by means of TFTP	**tftp get** *//A.A.A.A/xxx.yyy mmm.nnn*

1.4.4 Upload Files by means of TFTP

To upload a file, the client sends a request to the TFTP server and then transmits data to it and receives the acknowledgement from it. You can use the following commands to upload files.

Perform the following configuration in system view.

Table 1-17 Upload files by means of TFTP

Operation	Command
Upload files by means of TFTP	**tftp put** *mmm.nnn //A.A.A.A/xxx.yyy*

1.4.5 TFTP Client Configuration Example

I. Networking requirement

The switch serves as TFTP client and the remote PC as TFTP server. Authorized TFTP directory is set on the TFTP server. The IP address of a VLAN interface on the switch is 1.1.1.1, and that of the PC is 2.2.2.2. The interface on the switch connecting the PC belong to the same VLAN.

The switch application switch.app is stored on the PC. Using TFTP, the switch can download the switch.app from the remote TFTP server and upload the vrpcfg.txt to the TFTP server under the switch directory for backup purpose.

II. Networking diagram

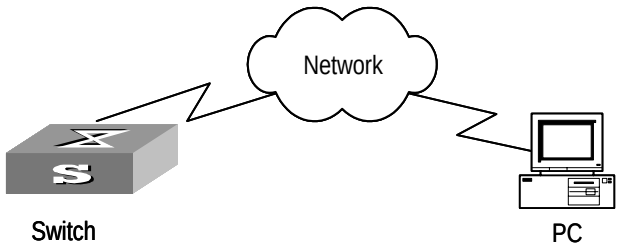


Figure 1-5 Networking for TFTP configuration

III. Configuration procedure

1) Start TFTP server on the PC and set authorized TFTP directory.
2) Configure the switch

Log into the switch (locally through the Console port or remotely using Telnet).

```
<Quidway>
```

Caution:

If the flash memory of the switch is not enough, you need to first delete the existing programs in the flash memory and then upload the new ones.

Enter system view and download the switch.app from the TFTP server to the flash memory of the switch.

```
<Quidway> system-view
[Quidway]
```

Configure IP address 1.1.1.1 for the VLAN interface, ensure the port connecting the PC is also in this VALN (VLAN 1 in this example).

```
[Quidway] interface vlan 1
[Quidway-vlan-interface1] ip address 1.1.1.1 255.255.255.0
[Quidway-vlan-interface1] quit
```

Upload the vrpcfg.txt to the TFTP server.

```
[Quidway] tftp  put vrpcfg.txt //1.1.1.2/vrpcfg.txt
```

Download the switch.app from the TFTP server.

```
[Quidway] tftp get //1.1.1.2/switch.app switch.app
```

Use the **boot boot-loader** command to specify the downloaded program as the application at the next login and reboot the switch.

```
<Quidway> boot boot-loader switch.app
<Quidway> reboot
```

Chapter 2 MAC Address Table Management

2.1 MAC Address Table Management Overview

An Ethernet Switch maintains a MAC address table for fast forwarding packets. A table entry includes the MAC address of a device and the port ID of the Ethernet switch connected to it. The dynamic entries (not configured manually) are learned by the Ethernet switch. The Ethernet switch learns a MAC address in the following way: after receiving a data frame from a port (assumed as port A), the switch analyzes its source MAC address (assumed as MAC_SOURCE) and considers that the packets destined at MAC_SOURCE can be forwarded via the port A. If the MAC address table contains the MAC_SOURCE, the switch will update the corresponding entry, otherwise, it will add the new MAC address (and the corresponding forwarding port) as a new entry to the table.

The system forwards the packets whose destination addresses can be found in the MAC address table directly through the hardware and broadcasts those packets whose addresses are not contained in the table. The network device will respond after receiving a broadcast packet and the response contains the MAC address of the device, which will then be learned and added into the MAC address table by the Ethernet switch. The consequent packets destined the same MAC address can be forwarded directly thereafter. If the MAC address cannot be found even after broadcasting the packet, the switch will drop it and notify the transmitter that the packet can not arrive at the destination.

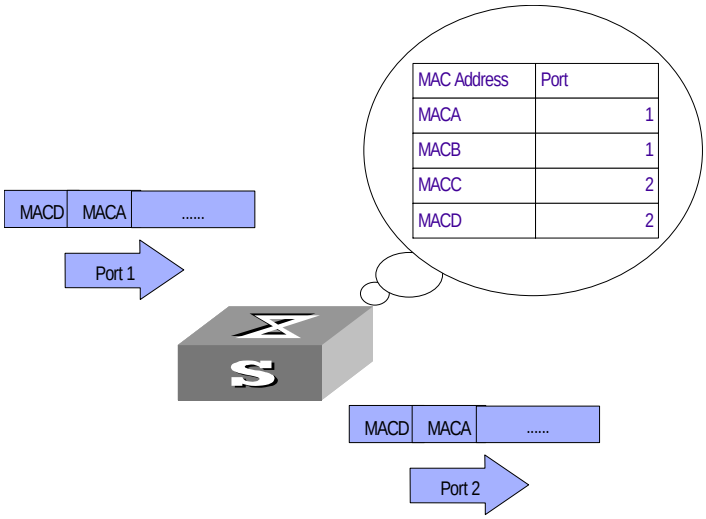


Figure 2-1 The Ethernet switch forwards packets with MAC address table

The Ethernet switch also provides the function of MAC address aging. If the switch receives no packet for a period of time, it will delete the related entry from the MAC address table. However, this function takes no effect on the static MAC addresses.

You can configure (add or modify) the MAC address entries manually according to the actual networking environment. The entries can be static ones or dynamic ones.

2.2 MAC Address Table Configuration

MAC address table management includes:

- Set MAC Address Table Entries
- Set MAC Address Aging Time
- Set the Max Count of MAC Address Learned by a Port

2.2.1 Set MAC Address Table Entries

Administrators can manually add, modify, or delete the entries in MAC address table according to the actual needs. They can also delete all the (unicast) MAC address table entries related to a specified port or delete a specified type of entries, such as dynamic entries or static entries.

You can use the following commands to add, modify, or delete the entries in MAC address table.

Perform the following configuration in system view.

Table 2-1 Set MAC address table entries

Operation	Command
Add/Modify an address entry	**mac-address** { **static** | **dynamic** } *hw-addr* **interface** { *interface-name* | *interface-type interface-num* } **vlan** *vlan-id*
Delete an address entry	**undo mac-address** [**static** | **dynamic**] [[*hw-addr*] **interface** [*interface-name* | *interface-type interface-num*] **vlan** *vlan-id*]

When deleting the dynamic address table entries, the learned entries will be deleted simultaneously.

2.2.2 Set MAC Address Aging Time

The setting of an appropriate aging time can effectively implement the function of MAC address aging. 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.

You can use the following commands to set the MAC address aging time for the system.

Perform the following configuration in system view.

Table 2-2 Set the MAC address aging time for the system

Operation	Command
Set the dynamic MAC address aging time	**mac-address timer** { **aging** *age* | **no-aging** }
Restore the default MAC address aging time	**undo mac-address timer aging**

In addition, this command takes effect on all the ports. However the address aging only functions on the dynamic addresses (the learned or configured as age entries by the user).

By default, the *aging-time* is 300 seconds. With the **no**-**aging** parameter, the command performs no aging on the MAC address entries.

2.2.3 Set the Max Count of MAC Address Learned by a Port

With the address learning function, an Ethernet switch can learn new MAC addresses. After received a packet destined some already learned MAC address, the switch will forward it directly with the hardware, instead of broadcasting. But Too many MAC address items learned by a port will affect the switch operation performance.

User can control the MAC address items learned by a port through setting the max count of MAC address learned by a port. If user set the max count value of a port as *count*, the port will not learn new MAC address items when the count of MAC address items reaches *count*.

You can use the following commands to set the max count of MAC address learned by a port.

Perform the following configuration in Ethernet port view.

Table 2-3 Set the Max Count of MAC Address Learned by a Port

Operation	Command
Set the Max Count of MAC Address Learned by a Port	**mac-address max-mac-count** *count*
Restore the default Max Count of MAC Address Learned by a Port	**undo mac-address max-mac-count**

By default, there is no limit to the MAC addresses learned via the Ethernet port.

2.3 Display and Debug MAC Address Table

After the above configuration, execute **display** command in any view to display the running of the MAC address table configuration, and to verify the effect of the configuration.

Table 2-4 Display and debug MAC address table

Operation	Command
Display the information in the address table	**display mac-address** [*mac-addr* [**vlan** *vlan-id*] | [**static** | **dynamic**] [**interface** { *interface-name* | *interface-type interface-num* }] [**vlan** *vlan-id*] [**count**]]
Display the aging time of dynamic address table entries	**display mac-address aging-time**

2.4 MAC Address Table Management Configuration Example

I. Networking requirements

The user logs in the switch via the Console port to configure the address table management. It is required to set the address aging time to 500s and add a static address 00e0-fc35-dc71 to Ethernet 0/2 in vlan1.

II. Networking diagram

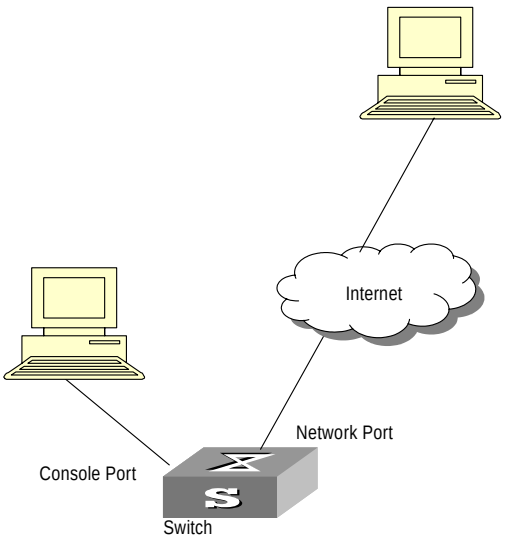


Figure 2-2 Typical configuration of address table management

III. Configuration procedure

Enter the system view of the switch.

```
<Quidway> system-view
```

Add a MAC address (specify the native VLAN, port and state).

```
[Quidway] mac-address static 00e0-fc35-dc71 interface ethernet 0/2 vlan 1
```

Set the address aging time to 500s.

```
[Quidway] mac-address timer aging 500
```

Display the MAC address configurations in any view.

```
[Quidway] display mac-address interface ethernet 0/2
MAC ADDR              VLAN ID   STATE     PORT INDEX    AGING TIME
00-e0-fc-35-dc-71     1         Static    Ethernet0/2   NOAGED
00-e0-fc-17-a7-d6     1         Learned   Ethernet0/2   AGING
00-e0-fc-5e-b1-fb     1         Learned   Ethernet0/2   AGING
00-e0-fc-55-f1-16     1         Learned   Ethernet0/2   AGING
---  4 mac address(es) found on port Ethernet0/2 ---
```

Chapter 3 Device management

3.1 Device Management Overview

With the device management function, the Ethernet Switch can display the current running state and event debugging information about the slots, thereby implementing the maintenance and management of the state and communication of the physical devices. In addition, there is a command available for rebooting the system, when some function failure occurs.

The device management configuration task is simple. As far as a user concerned, it is mainly the display and debug the device management.

3.2 Device Management Configuration

The device management configuration includes:

- Reboot Ethernet switch
- Designate the APP adopted when booting the Ethernet switch next time
- Upgrade BootROM

3.2.1 Reboot Ethernet Switch

It would be necessary for users to reboot the Ethernet switch when failure occurs.

Perform the following configuration in user view.

Table 3-1 Reboot Ethernet switch

Operation	Command
Reboot the whole system	**reboot**

3.2.2 Designate the APP Adopted When Booting the Ethernet Switch Next Time

In the case that there are several APPs in the Flash Memory, you can use this command to designate the APP adopted when booting the Ethernet switch next time.

Perform the following configuration in user view.

Table 3-2 Designate the APP adopted when booting the Ethernet switch next time

Operation	Command
Designate the APP adopted when booting the Ethernet switch next time	**boot boot-loader** *file-url*

3.2.3 Upgrade BootROM

You can use this command to upgrade the BootROM with the BootROM program in the Flash Memory. This configuration task facilitates the remote upgrade. You can upload the BootROM program file from a remote end to the switch via FTP and then use this command to upgrade the BootROM.

Perform the following configuration in user view.

Table 3-3 Upgrade BootROM

Operation	Command
Upgrade BootROM	**boot bootrom** *file-url*

3.3 Display and Debug Device Management Configuration

After the above configuration, execute **display** command in any view to display the running of the Device management configuration, and to verify the effect of the configuration.

Table 3-4 Display and debug Device management configuration

Operation	Command
Display the APP to be applied when rebooting the switch.	**display boot-loader**
Display the module types and running states of each slot	**display device**
Display the busy status of CPU	**display cpu**
Display the Used status of switch memory	**display memory** [**slot** *slot-number*]

Chapter 4 System Maintenance and Debugging

4.1 Basic System Configuration

4.1.1 Set Name for Switch

Perform the operation of **sysname** command in the system view.

Table 4-1 set name for Switch

Operation	Command
Set the switch name	**sysname** *sysname*
Restore switch name to default value	**undo sysname**

4.1.2 Set the System Clock

Perform the operation of **clock datetime** command in the user view.

Table 4-2 Set the system clock

Operation	Command
Set the system clock	**clock datetime** *HH:MM:SS YYYY/MM/DD*

4.1.3 Set the Time Zone

You can configure the name of the local time zone and the time difference between the local time and the standard Universal Time Coordinated (UTC).

Perform the following operations in the user view.

Table 4-3 Setting the time zone

Operation	Command
Set the local time	**clock timezone** *zone_name* { **add** | **minus** } *HH:MM:SS*
Restore to the default UTC time zone	**undo clock timezone**

By default, the UTC time zone is adopted.

4.1.4 Set the Summer Time

You can set the name, starting and ending time of the summer time.

Perform the following operations in the user view.

Table 4-4 Setting the summer time

Operation	Command
Set the name and range of the summer time	**clock summer-time** *zone_name* { **one-off** | **repeating** } *start-time start-date end-time end-date offset-time*
Remove the setting of the summer time	**undo clock summer-time**

By default, the summer time is not set.

4.2 Display the State and Information of the System

The **display** commands can be classified as follows according to their functions.

- Commands for displaying the system configuration information
- Commands for displaying the system running state
- Commands for displaying the system statistics information

For the **display** commands related to each protocols and different ports, refer to the relevant chapters. The following **display** commands are used for displaying the system state and the statistics information.

Perform the following operations in any view.

Table 4-5 The **display** commands of the system

Operation	Command
Display the system clock	**display clock**
Display the system version	**display version**
Display the terminal user	**display users** [**all**]
Display the saved-configuration	**display saved-configuration**
Display the current-configuration	**display current-configuration** [**controller** | **interface** *interface-type* [*interface-number*] | **configuration** [*configuration*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
Display the state of the debugging	**display debugging** [**interface** { *interface-name* | *interface-type interface-number* }] [*module-name*]

4.3 System Debugging

4.3.1 Enable/Disable the Terminal Debugging

The Ethernet switch provides various ways for debugging most of the supported protocols and functions, which can help you diagnose and address the errors.

The following switches can control the outputs of the debugging information:

- Protocol debugging switch controls the debugging output of a protocol.
- Terminal debugging switch controls the debugging output on a specified user screen.

The figure below illustrates the relationship between two switches.

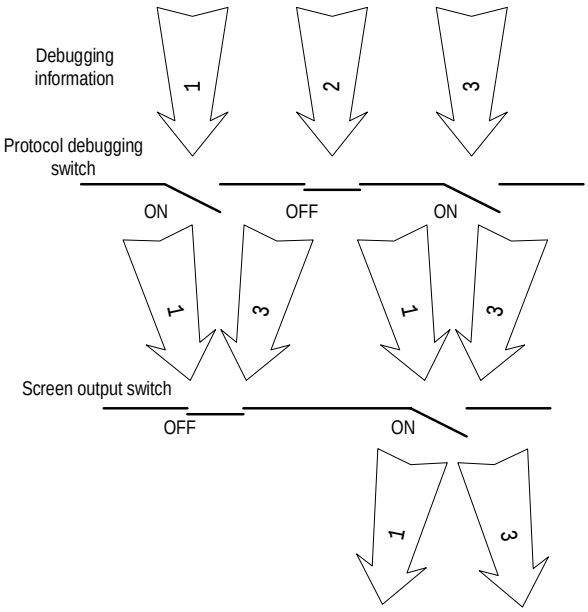


Figure 4-1 Debug output

You can use the following commands to control the above-mentioned debugging.

Perform the following operations in user view.

Table 4-6 Enable/Disable the debugging

Operation	Command
Enable the protocol debugging	**debugging** { **all** | *module-name* [*debugging-option*] }
Disable the protocol debugging	**undo debugging** { **all** | { *protocol-name* | *function-name* } [*debugging-option*] }
Enable the terminal debugging	**terminal debugging**
Disable the terminal debugging	**undo terminal debugging**

For more about the usage and format of the debugging commands, refer to the relevant chapters.

Note:

Since the debugging output will affect the system operating efficiency, do not enable the debugging without necessity, especially use the **debugging all** command with caution. When the debugging is over, disable all the debugging.

4.3.2 Display Diagnostic Information

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.

You can perform the following operations in any view.

Table 4-7 display diagnostic information

Operation	Command
display diagnostic information	**display diagnostic-information**

4.4 Testing Tools for Network Connection

I. ping

The **ping** command can be used to check the network connection and if the host is reachable.

Perform the following operation in any view.

Table 4-8 The **ping** command

Operation	Command
Support IP ping	**ping** [-**a** *ip-address*] [**-c** *count*] [**-d**] [-**h** *ttl*] [-**i** {*interface-type interface-num* | *interface-name* }] [**ip**] [**-n**] [**- p** *pattern*] [**-q**] [**-r**] [**-s** *packetsize*] [**-t** *timeout*] [**-tos** *tos*] [**-v**] *host*

The output of the command includes:

- The response to each ping message. If no response packet is received when time is out, ”Request time out” information appears. Otherwise, the data bytes, the

packet sequence number, TTL, and the round-trip time of the response packet will be displayed.

- The final statistics, including the number of the packets the switch sent out and received, the packet loss ratio, the round-trip time in its minimum value, mean value and maximum value.

II. tracert

The **tracert** is used for testing the gateways passed by the packets from the source host to the destination one. It is mainly used for checking if the network is connected and analyzing where the fault occurs in the network.

The execution process of tracert is described as follows: Send a packet with TTL value as 1 and the first hop sends back an ICMP error message indicating that the packet cannot be sent, for the TTL is timeout. Re-send the packet with TTL value as 2 and the second hop returns the TTL timeout message. The process is carried over and over until the packet reaches the destination. The purpose to carry out the process is to record the source address of each ICMP TTL timeout message, so as to provide the route of an IP packet to the destination.

Perform the following operation in any view.

Table 4-9 The **tracert** command

Operation	Command
Trace route	**tracert** [**-a** *source-IP*] [**-f** *first-TTL*] [**-m** *max-TTL*] [**-p** *port*] [**-q** *nqueries*] [**-w** *timeout*] *string*

4.5 Logging Function

4.5.1 Introduction to Info-center

The Info-center is an indispensable part of the Ethernet switch. It serves as an information center of the system software modules. The logging system is responsible for most of the information outputs, and it also makes detailed classification to filter the information efficiently. Coupled with the debugging program, the info-center provides powerful support for the network administrators and the R&D personnel to monitor the operating state of networks and diagnose network failures.

When the log information is output to terminal or log buffer, the following parts will be included:

```
%Timestamp Sysname Module name/Severity/Digest: Content
```

For example:

```
%Jun  7 05:22:03 2003 Quidway IFNET/6/UPDOWN:Line protocol on interface
Ethernet0/2, changed state to UP
```

When the log information is output to info-center, the first part will be “<Priority>”.

For example:

```
<187>Jun  7 05:22:03 2003 Quidway IFNET/6/UPDOWN:Line protocol on interface
Ethernet0/2, changed state to UP
```

The description of the components of log information is as follows:

1) Priority

The priority is computed according to following formula: facility*8+severity-1. The default value for the facility is 23. The range of severity is 1~8, and the severity will be introduced in separate section.

The value of facility can be set by command **info-center loghost**, .local1 to local7 corresponding to 16 to 23 respectively, for detailed information, refer to RFC3164 (The BSD syslog Protocol).

Notice: Priority is only effective when information is send to loghost. There is no character between priority and timestamp.

2) Timestamp

If the logging information is send to the log host, the default format of timestamp is date, and it can be changed to boot format or none format through the command:

info-center timestamp log { date | boot | none }

The date format of timestamp is "mm dd hh:mm:ss yyyy".

"mm" is month field, such as: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.

"dd" is day field, if the day is little than 10th, one blank should be added, such as " 7".

"hh:mm:ss" is time field, "hh" is from 00 to 23, "mm" and "ss" are from 00 to 59.

"yyyy" is year field.

If changed to boot format, it represents the milliseconds from system booting. Generally, the data is so big that we use two 32 bits integers, and separated with a dot '.'.

For example:

```
<189>0.166970 Quidway IFNET/6/UPDOWN:Line protocol on interface Ethernet0/2,
changed state to UP
```

It means that 166970ms (0*2^32+166970) has passed from system booting.

If changed to none format, the timestamp field is not present in logging information.

Notice: There is a blank between timestamp and sysname. If the timestamp is none format, there is a blank between priority and sysname.

3) Sysname

The sysname is the host name, the default value is "Quidway".

User can change the host name through **sysname** command.

Notice: There is a blank between sysname and module name.

4) Module name

The module name is the name of module which create this logging information, the following sheet list some examples:

Table 4-10 Module names in logging information

Module name	Description
BGP	Border Gateway Protocol
CFM	Configuration File Management
HWCM	Huawei Configuration Mib
IFNET	Interface Management
IP	Internet Protocol
NTP	Network Time Protocol
OSPF	Open Shortest Path First
SNMP	Simple Network Management Protocol

Notice: There is a slash ('/') between module name and severity.

5) Severity

Switch information falls into three categories: log information, debugging information and trap information. The info-center classifies every kind of information into 8 severity or urgent levels. The log filtering rule is that the system prohibits outputting the information whose severity level is greater than the set threshold. The more urgent the logging packet is, the smaller its severity level is. The level represented by “emergencies” is 0, and that represented by ”debugging” is 7. Therefore, when the threshold of the severity level is “debugging”, the system will output all the information.

Definition of severity in logging information is as followed.

Table 4-11 Info-center-defined severity

Severity	Description
emergencies	The extremely emergent errors
alerts	The errors that need to be corrected immediately.
critical	Critical errors
errors	The errors that need to be concerned but not critical
warnings	Warning, there might exist some kinds of errors.
notifications	The information should be concerned.
informational	Common prompting information

Severity	Description
debugging	Debugging information

Notice: There is a slash between severity and digest.

6) Digest

The digest is abbreviation, it represent the abstract of contents.

Notice: There is a colon between digest and content.

7) Content

It is the contents of logging information.

4.5.2 Info-center Configuration

Switch supports 6 output directions of information.

The system assigns a channel in each output direction by default. See the table below.

Table 4-12 Numbers and names of the channels for log output

Output direction	Channel number	Default channel name
Console	0	console
Monitor	1	monitor
Info-center loghost	2	loghost
Trap buffer	3	trapbuf
Logging buffer	4	logbuf
snmp	5	snmpagent

Note:

The settings in the six directions are independent from each other. The settings will take effect only after enabling the information center.

The info-center of Ethernet Switch has the following features:

- Support to output log in six directions, i.e., Console, monitor to Telnet terminal, logbuf, loghost, trapbuf, and SNMP.
- The log is divided into 8 levels according to the significance and it can be filtered based on the levels.
- The information can be classified in terms of the source modules and the information can be filtered in accordance with the modules.
- The output language can be selected between Chinese and English.

1) Sending the configuration information to loghost.

Table 4-13 Sending the configuration information to loghost

Device	Configuration	Default value	Configuration description
Switch	Enable info-center	By default, info-center is enabled.	Other configurations are valid only if the info-center is enabled.
	Set the information output direction to loghost	-	The configuration about the loghost on the switch and that on loghost must be the same; otherwise the information cannot be sent to the loghost correctly.
	Set information source	-	You can define which modules and information to be sent out and the time-stamp format of information, and so on. You must turn on the switch of the corresponding module before defining output debugging information.
Loghost	Refer to configuration cases for related log host configuration	-	-

2) Sending the configuration information to the console terminal.

Table 4-14 Sending the configuration information to the console terminal.

Device	Configuration	Default value	Configuration description
Switch	Enable info-center	By default, info-center is enabled.	Other configurations are valid only if the info-center is enabled.
	Set the information output direction to Console	-	-
	Set information source	-	You can define which modules and information to be sent out and the time-stamp format of information, and so on. You must turn on the switch of the corresponding module before defining output debugging information.
	Enable terminal display function	-	You can view debugging information after enabling terminal display function

3) Sending the configuration information to monitor terminal

Table 4-15 Sending the configuration information to monitor terminal

Device	Configuration	Default value	Configuration description
Switch	Enable info-center	By default, info-center is enabled.	Other configurations are valid only if the info-center is enabled.
	Set the information output direction to monitor	-	-
	Set information source	-	You can define which modules and information to be sent out and the time-stamp format of information, and so on. You must turn on the switch of the corresponding module before defining output debugging information.
	Enable the terminal display function and this function for the corresponding information	-	For Telnet terminal and dumb terminal, to view the information, you must enable the current terminal display function using the **terminal monitor** command.

4) Sending the configuration information to log buffer.

Table 4-16 Sending the configuration information to log buffer

Device	Configuration	Default value	Configuration description
Switch	Enable info-center	By default, info-center is enabled.	Other configurations are valid only if the info-center is enabled.
	Set the information output direction to logbuffer	-	You can configure the size of the log buffer at the same time.
	Set information source	-	You can define which modules and information to be sent out and the time-stamp format of information, and so on. You must turn on the switch of the corresponding module before defining output debugging information.

5) Sending the configuration information to trap buffer.

Table 4-17 Sending the configuration information to trap buffer

Device	Configuration	Default value	Configuration description
Switch	Enable info-center	By default, info-center is enabled.	Other configurations are valid only if the info-center is enabled.
	Set the information output direction to trapbuffer	-	You can configure the size of the trap buffer at the same time.
	Set information source	-	You can define which modules and information to be sent out and the time-stamp format of information, and so on. You must turn on the switch of the corresponding module before defining output debugging information.

6) Sending the configuration information to SNMP

Table 4-18 Sending the configuration information to SNMP

Device	Configuration	Default value	Configuration description
Switch	Enable info-center	By default, info-center is enabled.	Other configurations are valid only if the info-center is enabled.
	Set the information output direction to SNMP	-	-
	Set information source	-	You can define which modules and information to be sent out and the time-stamp format of information, and so on. You must turn on the switch of the corresponding module before defining output debugging information.
	Configuring SNMP features	-	See Chapter 5 SNMP Configuration
Network management workstation	The same as the SNMP configuration of the switch	-	-

7) Turn on/off the information synchronization switch in Fabric

Table 4-19 Turn on/off the information synchronization switch in Fabric

Device	Configuration	Default value	Configuration description
Switch	Enable info-center	By default, info-center is enabled.	Other configurations are valid only if the info-center is enabled.
	Set the information output direction to SNMP	By default, switches of master log in Fabric, debugging and trap information synchronization are turned on, so as log and strap information synchronization switches in other switches.	This configuration can keep log information, debugging information and trap information in Fabric in every switch synchronized.

4.5.3 Sending the Configuration Information to Loghost

To send configuration information to loghost, follow the steps below:

1) Enabling info-center

Perform the following operation in system view.

Table 4-20 Enable/disable info-center

Operation	Command
Enable info-center	**info-center enable**
Disable info-center	**undo info-center enable**

Note:

Info-center is enabled by default. After info-center is enabled, system performances are affected when the system processes much information because of information classification and outputting.

2) Configuring to output information to loghost

Perform the following operation in system view.

Table 4-21 Configuring to output information to loghost

Operation	Command
Output information to loghost	**info-center loghost** *host-ip-addr* [**channel** { *channel-number* | *channel-name* }] [**facility** *local-number*] [**language** { **chinese** | **english** }]

Operation	Command
Cancel the configuration of outputting information to loghost	**undo info-center loghost** *host-ip-addr*

Note:

Ensure to enter the correct IP address using the **info-center loghost** command to configure loghost IP address. If you enter a loopback address, the system prompts of invalid address appears.

3) Configuring information source on the switch

By this configuration, you can define the information that sent to console terminal is generated by which modules, information type, information level, and so on.

Perform the following operation in system view.

Table 4-22 Defining information source

Operation	Command
Define information source	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** }* { **level** *severity* | **state** *state* }*]
Cancel the configuration of information source	**undo info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* }

modu-name specifies the module name; **default** represents all the modules; **level** refers to the severity levels; *severity* specifies the severity level of information. The information with the level below it will not be output. *channel-number* specifies the channel number and *channel-name* specifies the channel name.

When defining the information sent to the loghost, *channel-number* or *channel-name* must be set to the channel that corresponds to loghost direction.

Every channel has been set with a default record, whose module name is **default** and the module number is 0xffff0000. However, for different channels, the default record may have different default settings of log, trap and debugging. When there is no specific configuration record for a module in the channel, use the default one.

Note:

If you want to view the debugging information of some modules on the switch, you must select **debugging** as the information type when configuring information source, meantime using the **debugging** command to turn on the debugging switch of those modules.

You can use the following commands to configure log information, debugging information and the time-stamp output format of trap information.

Perform the following operation in system view:

Table 4-23 Configuring the output format of time-stamp

Operation	Command
Configure the output format of the time-stamp	**info-center timestamp** { **log** | **trap** | **debugging** } { **boot** | **date** | **none** }
Output time-stamp is disabled	**undo info-center timestamp** { **log** | **trap** | **debugging** }

4) Configuring loghost

The configuration on the loghost must be the same with that on the switch. For related configuration, see the configuration examples in the later part.

4.5.4 Sending the Configuration Information to Console terminal

To send configuration information to console terminal, follow the steps below:

1) Enabling info-center

Perform the following operation in system view.

Table 4-24 Enable/disable info-center

Operation	Command
Enable info-center	**info-center enable**
Disable info-center	**undo info-center enable**

Note:

Info-center is enabled by default. After info-center is enabled, system performances are affected when the system processes much information because of information classification and outputting.

2) Configuring to output information to console terminal

Perform the following operation in system view.

Table 4-25 Configuring to output information to console terminal

Operation	Command
Output information to Console	**info-center console channel**{ *channel-number* | *channel-name* }
Cancel the configuration of outputting information to Console	**undo info-center console channel**

3) Configuring information source on the switch

By this configuration, you can define the information that sent to console terminal is generated by which modules, information type, information level, and so on.

Perform the following operation in system view:

Table 4-26 Defining information source

Operation	Command
Define information source	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** }* { **level** *severity* | **state** *state* }*]
Cancel the configuration of information source	**undo info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* }

modu-name specifies the module name; **default** represents all the modules; **level** refers to the severity levels; *severity* specifies the severity level of information. The information with the level below it will not be output. *channel-number* specifies the channel number and *channel-name* specifies the channel name.

When defining the information sent to the console terminal, *channel-number* or *channel-name* must be set to the channel that corresponds to Console direction.

Every channel has been set with a default record, whose module name is **default** and the module number is 0xffff0000. However, for different channels, the default record may have different default settings of log, trap and debugging. When there is no specific configuration record for a module in the channel, use the default one.

Note:

If you want to view the debugging information of some modules on the switch, you must select **debugging** as the information type when configuring information source, meantime using the **debugging** command to turn on the debugging switch of those modules.

You can use the following commands to configure log information, debugging information and the time-stamp output format of trap information.

Perform the following operation in system view:

Table 4-27 Configuring the output format of time-stamp

Operation	Command
Configure the output format of the time-stamp	**info-center timestamp** { **log** | **trap** | **debugging** } { **boot** | **date** | **none** }
Output time-stamp is disabled	**undo info-center timestamp** { **log** | **trap** | **debugging** }

4) Enable terminal display function

To view the output information at the console terminal, you must first enable the corresponding log, debugging and trap information functions at the switch.

For example, if you have set the log information as the information sent to the console terminal, now you need to use the **terminal logging** command to enable the terminal display function of log information on the switch, then you can view the information at the console terminal.

Perform the following operation in user view:

Table 4-28 Enabling terminal display function

Operation	Command
Enable terminal display function of debugging information	**terminal debugging**
Disable terminal display function of debugging information	**undo terminal debugging**
Enable terminal display function of log information	**terminal logging**
Disable terminal display function of log information	**undo terminal logging**
Enable terminal display function of trap information	**terminal trapping**
Disable terminal display function of trap information	**undo terminal trapping**

4.5.5 Sending the Configuration Information to Telnet Terminal or Dumb Terminal

To send configuration information to Telnet terminal or dumb terminal, follow the steps below:

1) Enabling info-center

Perform the following operation in system view.

Table 4-29 Enable/disable Info-center

Operation	Command
Enable info-center	**info-center enable**
Disable info-center	**undo info-center enable**

Note:

Info-center is enabled by default. After info-center is enabled, system performances are affected when the system processes much information because of information classification and outputting.

2) Configuring to output information to Telnet terminal or dumb terminal

Perform the following operation in system view.

Table 4-30 Configuring to output information to Telnet terminal or dumb terminal

Operation	Command
Output information to Telnet terminal or dumb terminal	**info-center monitor channel** { *channel-number* | *channel-name* }
Cancel the configuration of outputting information to Telnet terminal or dumb terminal	**undo info-center monitor channel**

3) Configuring information source on the switch

By this configuration, you can define the information that sent to Telnet terminal or dumb terminal is generated by which modules, information type, information level, and so on.

Perform the following operation in system view:

Table 4-31 Defining information source

Operation	Command
Define information source	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** }* { **level** *severity* | **state** *state* }*]
Cancel the configuration of information source	**undo info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* }

modu-name specifies the module name; **default** represents all the modules; **level** refers to the severity levels; *severity* specifies the severity level of information. The information with the level below it will not be output. *channel-number* specifies the channel number and *channel-name* specifies the channel name.

When defining the information sent to Telnet terminal or dumb terminal, *channel-number* or *channel-name* must be set to the channel that corresponds to Console direction.

Every channel has been set with a default record, whose module name is **default** and the module number is 0xffff0000. However, for different channels, the default record may have different default settings of log, trap and debugging. When there is no specific configuration record for a module in the channel, use the default one.

Note:

When there are more than one Telnet users or monitor users at the same time, some configuration parameters should be shared among the users, such as module-based filtering settings and severity threshold. When a user modifies these settings, it will be reflected on other clients.

Note:

If you want to view the debugging information of some modules on the switch, you must select **debugging** as the information type when configuring information source, meantime using the **debugging** command to turn on the debugging switch of those modules.

You can use the following commands to configure log information, debugging information and the time-stamp output format of trap information.

Perform the following operation in system view:

Table 4-32 Configuring the output format of time-stamp

Operation	Command
Configure the output format of the time-stamp	**info-center timestamp** { **log** | **trap** | **debugging** } { **boot** | **date** | **none** }
Output time-stamp is disabled	**undo info-center timestamp** { **log** | **trap** | **debugging** }

4) Enabling terminal display function

To view the output information at the Telnet terminal or dumb terminal, you must first enable the corresponding log, debugging and trap information functions at the switch.

For example, if you have set the log information as the information sent to the Telnet terminal or dumb terminal, now you need to use the **terminal logging** command to enable the terminal display function of log information on the switch, then you can view the information at the Telnet terminal or dumb terminal.

Perform the following operation in user view:

Table 4-33 Enabling terminal display function

Operation	Command
Enable terminal display function of log, debugging and trap information	**terminal monitor**
Disable terminal display function of the above information	**undo terminal monitor**
Enable terminal display function of debugging information	**terminal debugging**
Disable terminal display function of debugging information	**undo terminal debugging**
Enable terminal display function of log information	**terminal logging**
Disable terminal display function of log information	**undo terminal logging**
Enable terminal display function of trap information	**terminal trapping**
Disable terminal display function of trap information	**undo terminal trapping**

4.5.6 Sending the Configuration Information to Log Buffer

To send configuration information to log buffer, follow the steps below:

1) Enabling info-center

Perform the following operation in system view.

Table 4-34 Enabling/disabling info-center

Operation	Command
Enable info-center	**info-center enable**
Disable info-center	**undo info-center enable**

Note:

Info-center is enabled by default. After info-center is enabled, system performances are affected when the system processes much information because of information classification and outputting.

2) Configuring to output information to log buffer

Perform the following operation in system view.

Table 4-35 Configuring to output information to log buffer

Operation	Command
Output information to log buffer	**info-center logbuffer** [**channel** { *channel-number* | *channel-name* }] [**size** *buffersize*]
Cancel the configuration of outputting information to log buffer	**undo info-center logbuffer** [**channel** | **size**]

3) Configuring information source on the switch

By this configuration, you can define the information that sent to log buffer is generated by which modules, information type, information level, and so on.

Perform the following operation in system view:

Table 4-36 Defining information source

Operation	Command
Define information source	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** }* { **level** *severity* | **state** *state* }*]
Cancel the configuration of information source	**undo info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* }

modu-name specifies the module name; **default** represents all the modules; **level** refers to the severity levels; *severity* specifies the severity level of information. The

information with the level below it will not be output. *channel-number* specifies the channel number and *channel-name* specifies the channel name.

When defining the information sent to log buffer, *channel-number* or *channel-name* must be set to the channel that corresponds to Console direction.

Every channel has been set with a default record, whose module name is **default** and the module number is 0xffff0000. However, for different channels, the default record may have different default settings of log, trap and debugging. When there is no specific configuration record for a module in the channel, use the default one.

Note:

If you want to view the debugging information of some modules on the switch, you must select **debugging** as the information type when configuring information source, meantime using the **debugging** command to turn on the debugging switch of those modules.

You can use the following commands to configure log information, debugging information and the time-stamp output format of trap information.

Perform the following operation in system view:

Table 4-37 Configuring the output format of time-stamp

Operation	Command
Configure the output format of the time-stamp	**info-center timestamp** { **log** | **trap** | **debugging** } { **boot** | **date** | **none** }
Output time-stamp is disabled	**undo info-center timestamp** { **log** | **trap** | **debugging** }

4.5.7 Sending the Configuration Information to Trap Buffer

To send configuration information to trap buffer, follow the steps below:

1) Enabling info-center

Perform the following operation in system view.

Table 4-38 Enabling/disabling info-center

Operation	Command
Enable info-center	**info-center enable**
Disable info-center	**undo info-center enable**

Note:

Info-center is enabled by default. After info-center is enabled, system performances are affected when the system processes much information because of information classification and outputting.

2) Configuring to output information to trap buffer

Perform the following operation in system view.

Table 4-39 Configuring to output information to trap buffer

Operation	Command
Output information to trap buffer	**info-center trapbuffer** [**size** *buffersize*] [**channel** { *channel-number* | *channel-name* }]
Cancel the configuration of outputting information to trap buffer	**undo info-center trapbuffer** [**channel** | **size**]

3) Configuring information source on the switch

By this configuration, you can define the information that sent to trap buffer is generated by which modules, information type, information level, and so on.

Perform the following operation in system view:

Table 4-40 Defining information source

Operation	Command
Define information source	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** }* { **level** *severity* | **state** *state* }*]
Cancel the configuration of information source	**undo info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* }

modu-name specifies the module name; **default** represents all the modules; **level** refers to the severity levels; *severity* specifies the severity level of information. The information with the level below it will not be output. *channel-number* specifies the channel number and *channel-name* specifies the channel name.

When defining the information sent to trap buffer, *channel-number* or *channel-name* must be set to the channel that corresponds to Console direction.

Every channel has been set with a default record, whose module name is **default** and the module number is 0xffff0000. However, for different channels, the default record

may have different default settings of log, trap and debugging. When there is no specific configuration record for a module in the channel, use the default one.

Note:

If you want to view the debugging information of some modules on the switch, you must select **debugging** as the information type when configuring information source, meantime using the **debugging** command to turn on the debugging switch of those modules.

You can use the following commands to configure log information, debugging information and the time-stamp output format of trap information.

Perform the following operation in system view:

Table 4-41 Configuring the output format of time-stamp

Operation	Command
Configure the output format of the time-stamp	**info-center timestamp** { **log	trap**	**debugging** } { **boot**	**date**	**none** }
Output time-stamp is disabled	**undo info-center timestamp** { **log**	**trap**	**debugging** }

4.5.8 Sending the Configuration Information to SNMP Network Management

To send configuration information to SNMP NM, follow the steps below:

1) Enabling info-center

Perform the following operation in system view.

Table 4-42 Enabling/disabling info-center

Operation	Command
Enable info-center	**info-center enable**
Disable info-center	**undo info-center enable**

Note:

Info-center is enabled by default. After info-center is enabled, system performances are affected when the system processes much information because of information classification and outputting.

---

2) Configuring to output information to SNMP NM

Perform the following operation in system view.

Table 4-43 Configuring to output information to SNMP NM

Operation	Command
Output information to SNMP NM	**info-center snmp channel** { *channel-number* | *channel-name* }
Cancel the configuration of outputting information to SNMP NM	**undo info-center snmp channel**

3) Configuring information source on the switch

By this configuration, you can define the information that sent to SNMP NM is generated by which modules, information type, information level, and so on.

Perform the following operation in system view:

Table 4-44 Defining information source

Operation	Command
Define information source	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** }* { **level** *severity* | **state** *state* }*]
Cancel the configuration of information source	**undo info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* }

modu-name specifies the module name; **default** represents all the modules; **level** refers to the severity levels; *severity* specifies the severity level of information. The information with the level below it will not be output. *channel-number* specifies the channel number and *channel-name* specifies the channel name.

When defining the information sent to SNMP NM, *channel-number* or *channel-name* must be set to the channel that corresponds to Console direction.

Every channel has been set with a default record, whose module name is **default** and the module number is 0xffff0000. However, for different channels, the default record may have different default settings of log, trap and debugging. When there is no specific configuration record for a module in the channel, use the default one.

Note:

If you want to view the debugging information of some modules on the switch, you must select **debugging** as the information type when configuring information source, meantime using the **debugging** command to turn on the debugging switch of those modules.

You can use the following commands to configure log information, debugging information and the time-stamp output format of trap information.

Perform the following operation in system view:

Table 4-45 Configuring the output format of time-stamp

Operation	Command
Configure the output format of the time-stamp	**info-center timestamp** { **log** | **trap** | **debugging** } { **boot** | **date** | **none** }
Output time-stamp is disabled	**undo info-center timestamp** { **log** | **trap** | **debugging** }

4) Configuring of SNMP and network management workstation on the switch

You have to configure SNMP on the switch and the remote workstation to ensure that the information is correctly sent to SNMP NM. Then you can get correct information from network management workstation. SNMP configuration on switch refers to Chapter 5 SNMP Configuration.

4.5.9 Turn on/off the Information Synchronization Switch in Fabric

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.

1) Enable info-center

Perform the following operation in system view.

Table 4-46 Enable/disable info-center

Operation	Command
Enable info-center	**info-center enable**
Disable info-center	**undo info-center enable**

2) Turn on the information synchronization switch

Perform the following operation in system view.

Table 4-47 Turn on/off the information synchronization switch of every switch

Operation	Command
Turn on the information synchronization switch of the specified switch	**info-center switch-on** { *unit-id* | **master** | **all** } [**debugging** | **logging** | **trapping**]*
Turn off the information synchronization switch of the specified switch	**undo info-center switch-on** { *unit-id* | *master* | **all** } [**debugging** | **logging** | **trapping**]*

You can turn on/off the synchronization switch of the specified information on the specified switch as needed.

By default, the log, debugging and trap information synchronization switch of master in Fabric are all turned on. The log, debugging and trap information synchronization switch of other switches are turned on.

4.5.10 Displaying and Debugging Info-center

After the above configuration, performing the **display** command in any view, you can view the running state of the info-center. You also can authenticate the effect of the configuration by viewing displayed information. Performing the **reset** command in user view, you can clear statistics of info-center.

Perform the following operation in user view. The **display** command still can be performed in any view.

Table 4-48 Displaying and debugging info-center

Operation	Command
Display the content of information channel	**display channel** [*channel-number* | *channel-name*]
Display configuration of system log and memory buffer	**display info-center**
Clear information in memory buffer	**reset logbuffer**
Clear information in trap buffer	**reset trapbuffer**

4.5.11 Configuration examples of sending log to Unix loghost

I. Networking Requirement

The networking requirement are as follows:

- Sending the log information of the switch to Unix loghost
- The IP address of the loghost is 202.38.1.10
- The information with the severity level above informational will be sent to the loghost
- The output language is English
- The modules that allowed to output information are ARP and IP

II. Networking diagram

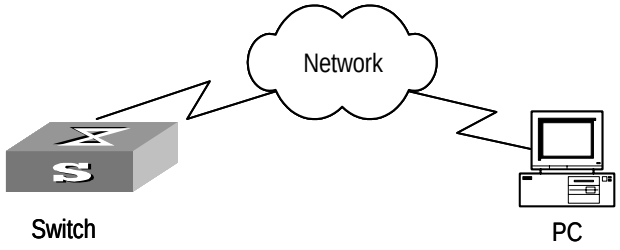


Figure 4-2 Schematic diagram of configuration

III. Configuration steps

1) Configuration on the switch

Enabling info-center

```
[Quidway] info-center enable
```

Set the host with the IP address of 202.38.1.10 as the loghost; set the severity level threshold value as informational, set the output language to English; set that the modules which are allowed to output information are ARP and IP.

```
[Quidway] info-center loghost 202.38.1.10 facility local4 language english
[Quidway] info-center source arp channel loghost log level informational
[Quidway] info-center source ip channel loghost log level informational
```

2) Configuration on the loghost

This configuration is performed on the loghost. The following example is performed on SunOS 4.0 and the operation on Unix operation system produced by other manufactures is generally the same to the operation on SunOS 4.0.

Step 1: Perform the following command as the super user (root).

```
# mkdir /var/log/Quidway
# touch /var/log/Quidway/information
```

Step 2: Edit file /etc/syslog.conf as the super user (root), add the following selector/actor pairs.

```
# Quidway configuration messages
local4.info     /var/log/Quidway/information
```

Note:

Note the following points when editing /etc/syslog.conf:

- The note must occupy a line and start with the character #.
- There must be a tab other than a space as the separator in selector/actor pairs.
- No redundant space after file name.
- The device name and the acceptant log information level specified in /etc/syslog.conf must be consistent with info-center loghost and info-center loghost a.b.c.d facility configured on the switch. Otherwise, the log information probably cannot be output to the loghost correctly.

Step 3: After the establishment of information (log file) and the revision of /etc/syslog.conf, you should send a HUP signal to syslogd (system daemon), through the following command, to make syslogd reread its configuration file /etc/syslog.conf.

```
# ps -ae | grep syslogd
147
# kill -HUP 147
```

After the above operation, the switch system can record information in related log files.

Note:

To configure facility, severity, filter and the file syslog.conf synthetically, you can get classification in great detail and filter the information.

4.5.12 Configuration examples of sending log to Linux loghost

I. Networking Requirement

The networking requirement are as follows:

- Sending the log information of the switch to Linux loghost
- The IP address of the loghost is 202.38.1.10
- The information with the severity level above informational will be sent to the loghost
- The output language is English

- All modules are allowed to output information

II. Networking diagram

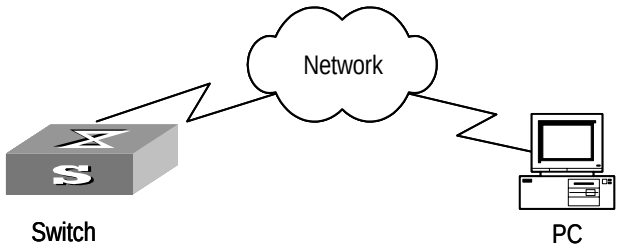


Figure 4-3 Schematic diagram of configuration

III. Configuration steps

1) Configuration steps

Enabling info-center

```
[Quidway] info-center enable
```

Set the host with the IP address of 202.38.1.10 as the loghost; set the severity level threshold value as informational, set the output language to English; set all the modules are allowed output information.

```
[Quidway] info-center loghost 202.38.1.10 facility local7 language english
[Quidway] info-center source default channel loghost log level informational
```

2) Configuration on the loghost

This configuration is performed on the loghost.

Step 1: Perform the following command as the super user (root).

```
# mkdir /var/log/Quidway
# touch /var/log/Quidway/information
```

Step 2: Edit file /etc/syslog.conf as the super user (root), add the following selector/actor pairs.

```
# Quidway configuration messages
local7.info     /var/log/Quidway/information
```

Note:

Note the following points when editing /etc/syslog.conf:

- The note must occupy a line and start with the character #.
- There must be a tab other than a space as the separator in selector/actor pairs.
- No redundant space after file name.
- The device name and the acceptant log information level specified in /etc/syslog.conf must be consistent with info-center loghost and info-center loghost a.b.c.d facility configured on the switch. Otherwise, the log information probably cannot be output to the loghost correctly.

Step 3: After the establishment of information (log file) and the revision of /etc/syslog.conf, you should view the number of syslogd (system daemon) through the following command, kill syslogd daemon and reuse -r option the start syslogd in daemon.

```
# ps -ae | grep syslogd
147
# kill -9 147
# syslogd -r &
```

Note:

For Linux loghost, you must ensure that syslogd daemon is started by -r option.

After the above operation, the switch system can record information in related log files.

Note:

To configure facility, severity, filter and the file syslog.conf synthetically, you can get classification in great detail and filter the information.

4.5.13 Configuration examples of sending log to console terminal

I. Networking Requirement

The networking requirement are as follows:

- Sending the log information of the switch to console terminal
- The information with the severity level above informational will be sent to the console terminal

- The output language is English

The modules that allowed to output information are ARP and IP

II. Networking diagram

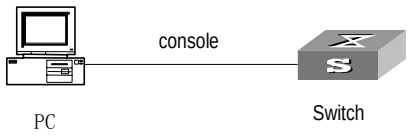


Figure 4-4 Schematic diagram of configuration

III. Configuration steps

1) Configuration on the switch

Enabling info-center

```
[Quidway] info-center enable
```

Configure console terminal log output; allow modules ARP and IP to output information; the severity level is restricted within the range of emergencies to informational.

```
[Quidway] info-center console channel console
[Quidway] info-center source arp channel console log level informational
[Quidway] info-center source ip channel console log level informational
```

Enabling terminal display function

```
<Quidway> terminal logging
```

Chapter 5 SNMP Configuration

5.1 SNMP Overview

By far, the Simple Network Management Protocol (SNMP) has gained the most extensive application in the computer networks. SNMP has been put into use and widely accepted as an industry standard in practice. It is used for ensuring the transmission of the management information between any two nodes. In this way, network administrators can easily search and modify the information on any node on the network. In the meantime, they can locate faults promptly and implement the fault diagnosis, capacity planning and report generating. SNMP adopts the polling mechanism and provides the most basic function set. It is most applicable to the small-sized, fast-speed and low-cost environment. It only requires the unverified transport layer protocol UDP; and is thus widely supported by many other products.

In terms of structure, SNMP can be divided into two parts, namely, Network Management Station and Agent. Network Management Station is the workstation for running the client program. At present, the commonly used NM platforms include Sun NetManager and IBM NetView. Agent is the server software operated on network devices. Network Management Station can send GetRequest, GetNextRequest and SetRequest messages to the Agent. Upon receiving the requests from the Network Management Station, Agent will perform Read or Write operation according to the message types, generate and return the Response message to Network Management Station. On the other hand, Agent will send Trap message on its own initiative to the Network Management Station to report the events whenever the device encounters any abnormalities such as new device found and restart.

5.2 SNMP Versions and Supported MIB

To uniquely identify the management variables of a device in SNMP messages, SNMP adopts the hierarchical naming scheme to identify the managed objects. It is like a tree. A tree node represents a managed object, as shown in the figure below. Thus the object can be identified with the unique path starting from the root.

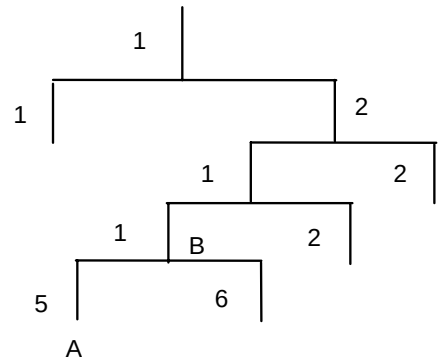


Figure 5-1 Architecture of the MIB tree

The MIB (Management Information Base) is used to describe the hierarchical architecture of the tree and it is the set defined by the standard variables of the monitored network device. In the above figure, the managed object B can be uniquely specified by a string of numbers {1.2.1.1}. The number string is the Object Identifier of the managed object.

The current SNMP Agent of Ethernet switch supports SNMP V1, V2C and V3. The MIBs supported are listed in the following table.

Table 5-1 MIBs supported by the Ethernet Switch

MIB attribute	MIB content	References
Public MIB	MIB II based on TCP/IP network device	RFC1213
	BRIDGE MIB	RFC1493
		RFC2675
	RIP MIB	RFC1724
	RMON MIB	RFC2819
	Ethernet MIB	RFC2665
	OSPF MIB	RFC1253
	IF MIB	RFC1573
Private MIB	DHCP MIB	
	QACL MIB	
	ADBM MIB	
	RSTP MIB	
	VLAN MIB	
	Device management	
	Interface management	

5.3 Configure SNMP

The main configuration of SNMP includes:

- Set community name
- Set the Method of Identifying and Contacting the Administrator
- Enable/Disable snmp Agent to Send Trap
- Set the Destination Address of Trap
- Set sysLocation
- Set the Engine ID of a Local or Remote Device
- Set/Delete an SNMP Group
- Set the Source Address of Trap
- Add/Delete a User to/from an SNMP Group
- Create/Update View Information or Deleting a View
- Set the Size of SNMP Packet Sent/Received by an Agent

5.3.1 Set Community Name

SNMP V1 and SNMPV2C adopt the community name authentication scheme. The SNMP message incompliant with the community name accepted by the device will be discarded. SNMP Community is named with a character string, which is called Community Name. The various communities can have read-only or read-write access mode. The community with read-only authority can only query the device information, whereas the community with read-write authority can also configure the device.

You can use the following commands to set the community name.

Perform the following configuration in system view.

Table 5-2 Set community name

Operation	Command
Set the community name and the access authority	**snmp-agent community** { **read** | **write** } *community-name* [[**mib-view** *view-name*] [**acl** *acl-list*]]
Remove the community name and the access authority	**undo snmp-agent community** *community-name*

5.3.2 Set the Method of Identifying and Contacting the Administrator

The sysContact is a management viable of the system group in MIB II. The content is the method of identifying and contacting the related personnel of the managed device.

You can use the following commands to set the method of identifying and contacting the administrators.

Perform the following configuration in system view.

Table 5-3 Set the method of identifying and contacting the administrator

Operation	Command
Set the method of identifying and contacting the administrator	**snmp-agent sys-info contact** *sysContact*
Restore the default method of identifying and contacting the administrator	**undo snmp-agent sys-info contact**

5.3.3 Enable/Disable SNMP Agent to Send Trap

The managed device transmits trap without request to the Network Management Station to report some critical and urgent events (such as restart).

You can use the following commands to enable or disable the managed device to transmit trap message.

Perform the following configuration in system view.

Table 5-4 Enable/Disable snmp agent to Send Trap

Operation	Command
Enable to send trap	**snmp-agent trap enable** [**standard** [**authentication**] [**coldstart**] [**linkdown**] [**linkup**] [**warmstart**]]
Disable to send trap	**undo snmp-agent trap enable** [**standard** [**authentication**] [**coldstart**] [**linkdown**] [**linkup**] [**warmstart**]]

5.3.4 Set the Destination Address of Trap

You can use the following commands to set or delete the destination address of the trap.

Perform the following configuration in system view.

Table 5-5 Set the destination address of trap

Operation	Command
Set the destination address of trap	**snmp-agent target-host trap address udp-domain** *host-addr* [**udp-port** *udp-port-number*] **params securityname** *community-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]]
Delete the destination address of trap	**undo snmp-agent target-host** *host-addr* **securityname** *community-string*

5.3.5 Set Lifetime of Trap Message

You can use the following command to set lifetime of Trap message. Trap message that exists longer than the set lifetime will be dropped.

Perform the following configuration in system view.

Table 5-6 Set the lifetime of Trap message

Operation	Command
Set lifetime of Trap message	**snmp-agent trap life** *seconds*
Restore lifetime of Trap message	**undo snmp-agent trap life**

By default, the lifetime of Trap message is 120 seconds.

5.3.6 Set SysLocation

The sysLocation is a management variable of the MIB system group, used for specifying the location of managed devices.

You can use the following commands to set the sysLocation.

Perform the following configuration in system view.

Table 5-7 Set sysLocation

Operation	Command
Set sysLocation	**snmp-agent sys-info location** *sysLocation*
Restore the default location of the Ethernet switch	**undo snmp-agent sys-info location**

By default, the *sysLocation* is specified as “Beijing China”.

5.3.7 Set SNMP Version

You can use the following commands to set the Set SNMP Version.

Perform the following configuration in system view.

Table 5-8 Set SNMP Version

Operation	Command
Set SNMP Version	**snmp-agent sys-info version** { { **v1** | **v2c** | **v3** } * | **all** }
Restore the default SNMP Version of the Ethernet switch	**undo snmp-agent sys-info version** { { **v1** | **v2c** | **v3** } * | **all** }

5.3.8 Set the Engine ID of a Local or Remote Device

You can use the following commands to set the engine ID of a local or remote device.

Perform the following configuration in system view.

Table 5-9 Set the engine ID of a local or remote device

Operation	Command
Set the engine ID of the device	**snmp-agent local-engineid** *engineid*
Restore the default engine ID of the device.	**undo snmp-agent local-engineid**

By default, the engine ID is expressed as enterprise No. + device information. The device information can be IP address, MAC address, or user-defined text.

5.3.9 Set/Delete an SNMP Group

You can use the following commands to set or delete an SNMP group.

Perform the following configuration in system view.

Table 5-10 Set/Delete an SNMP Group

Operation	Command
Setting an SNMP group	**snmp-agent group** { **v1** | **v2c** } *group-name* [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-list*] **snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-list*]
Deleting an SNMP group	**undo snmp-agent group** { **v1** | **v2c** } *group-name* **undo snmp-agent group v3** *group-name* [**authentication** | **privacy**]

5.3.10 Set the Source Address of Trap

You can use the following commands to set or remove the source address of the trap.

Perform the following configuration in system view.

Table 5-11 Set the source address of trap

Operation	Command
Set the Source Address of Trap	**snmp-agent trap source** *interface-name interface-num*
Remove the source address of trap	**undo snmp-agent trap source**

5.3.11 Add/Delete a User to/from an SNMP Group

You can use the following commands to add or delete a user to/from an SNMP group.

Perform the following configuration in system view.

Table 5-12 Add/Delete a user to/from an SNMP group

Operation	Command
Add a user to an SNMP group.	**snmp-agent usm-user** { **v1** | **v2c** } *username groupname* [**acl** *acl-list*] **snmp-agent usm-user v3** *username groupname* [**authentication-mode** { **md5** | **sha** } *authpassstring* [**privacy-mode** { **des56** *privpassstring* }]] [**acl** *acl-list*]
Delete a user from an SNMP group.	**undo snmp-agent usm-user** { **v1** | **v2c** } *username groupname* **undo snmp-agent usm-user v3** *username groupname* { **local** | **engineid** *engine-id* }

5.3.12 Create/Update View Information or Deleting a View

You can use the following commands to create, update the information of views or delete a view.

Perform the following configuration in system view.

Table 5-13 Create/Update view information or deleting a view

Operation	Command
Create/Update view information	**snmp-agent mib-view** { **included** | **excluded** } *view-name oid-tree*
Delete a view	**undo snmp-agent mib-view** *view-name*

5.3.13 Set the Size of SNMP Packet Sent/Received by an Agent

You can use the following commands to set the size of SNMP packet sent/received by an agent.

Perform the following configuration in system view.

Table 5-14 Set the size of SNMP packet sent/received by an agent

Operation	Command
Set the size of SNMP packet sent/received by an agent	**snmp-agent packet max-size** *byte-count*
Restore the default size of SNMP packet sent/received by an agent	**undo snmp-agent packet max-size**

The agent can receive/send the SNMP packets of the sizes ranging from 484 to 17940, measured in bytes. By default, the size of SNMP packet is 1500 bytes.

5.3.14 Disable SNMP Agent

To disable SNMP Agent, please Perform the following configuration in system view.

Table 5-15 Disable snmp agent

Operation	Command
Disable snmp agent	**undo snmp-agent**

If user disable NMP Agent, it will be enabled whatever **snmp-agent** command is configured thereafter.

5.4 Display and Debug SNMP

After the above configuration, execute **display** command in any view to display the running of the SNMP configuration, and to verify the effect of the configuration. Execute **debugging** command in user view to debug SNMP configuration.

Table 5-16 Display and debug SNMP

Operation	Command
Display the statistics information about SNMP packets	**display snmp-agent statistics**
Display the engine ID of the active device	**display snmp-agent** { **local-engineid** | **remote-engineid** }
Display the group name, the security mode, the states for all types of views, and the storage mode of each group of the switch.	**display snmp-agent group** [*group-name*]
Display the names of all users in the group user table	**display snmp-agent usm-user** [**engineid** *engineid*] [**group** *groupname*] [**username** *username*]
Display the current community name	**display snmp-agent community** [**read** | **write**]
Display the current MIB view	**display snmp-agent mib-view** [**exclude** | **include** | { **viewname** *mib-view* }]
Display the contact character string of the system	**display snmp-agent sys-info contact**
Display the location character string of the system	**display snmp-agent sys-info location**
Display the version character string of the system	**display snmp-agent sys-info version**

5.5 SNMP Configuration Example

I. Networking requirements

Network Management Station and the Ethernet switch are connected via the Ethernet. The IP address of Network Management Station is 129.102.149.23 and that of the VLAN interface on the switch is 129.102.0.1. Perform the following configurations on the switch: setting the community name and access authority, administrator ID, contact and switch location, and enabling the switch to sent trap packet.

II. Networking diagram

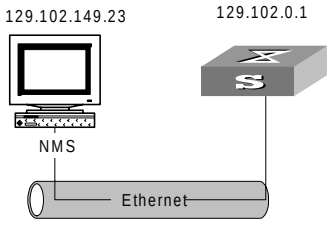


Figure 5-2 SNMP configuration example

III. Configuration procedure

Enter the system view.

```
<Quidway> system-view
```

Set the community name , group name and user.

```
[Quidway] snmp-agent sys-info version all
[Quidway] snmp-agent community write public
[Quidway] snmp-agent mib include internet 1.3.6.1
[Quidway] snmp-agent group v3 managev3group write internet
[Quidway] snmp-agent usm v3 managev3user managev3group
```

Set the VLAN interface 2 as the interface used by network management. Add port Ethernet 0/3 to the VLAN 2. This port will be used for network management. set the IP address of VLAN interface 2 as 129.102.0.1.

```
[Quidway] vlan 2
[Quidway-vlan2] port ethernet 0/3
[Quidway-vlan2] interface vlan 2
[Quidway-Vlan-interface2] ip address 129.102.0.1 255.255.255.0
```

Set the administrator ID, contact and the physical location of the Ethernet switch.

```
[Quidway] snmp-agent sys-info contact Mr.Wang-Tel:3306
[Quidway] snmp-agent sys-info location telephone-closet,3rd-floor
```

Enable SNMP agent to send the trap to Network Management Station whose ip address is 129.102.149.23. The SNMP community is public.

```
[Quidway] snmp-agent trap enable standard authentication
[Quidway] snmp-agent trap enable standard coldstart
[Quidway] snmp-agent trap enable standard linkup
[Quidway] snmp-agent trap enable standard linkdown
[Quidway] snmp-agent target-host trap address udp-domain 129.102.149.23
udp-port 5000 params securityname public
```

IV. Configure Network Management System

The Ethernet Switch supports Huawei's iManager Quidview NMS. Users can query and configure the Ethernet switch through the network management system. For more about it, refer to the manuals of Huawei's NM products.

Chapter 6 RMON Configuration

6.1 RMON Overview

Remote Network Monitoring (RMON) is a type of IETF-defined MIB. It is the most important enhancement to the MIB II standard. It mainly used for monitoring the data traffic on a segment and even on a whole network. It is one of the widely used Network Management standards by far.

RMON is implemented fully based on the SNMP architecture (which is one of its outstanding advantages) and compatible with the existing SNMP framework, and therefore it is unnecessary to adjust the protocol. RMON includes NMS and the Agent running on the network devices. On the network monitor or detector, RMON Agent tracks and accounts different traffic information on the segment connected to its port, such as the total number of packets on a segment in a certain period of time or that of the correct packets sent to a host. ROMN helps the SNMP monitor the remote network device more actively and effectively, which provides a highly efficient means for the monitoring of the subnet operations. RMON can reduce the communication traffic between the NMS and the agent, thus facilitates an effective management over the large interconnected networks.

RMON allows multiple monitors. It can collect data in two ways.

- One is to collect data with a special RMON probe. NMS directly obtains the management information from the RMON probe and controls the network resource. In this way, it can obtain all the information of RMON MIB
- Another way is to implant the RMON Agent directly into the network devices (e.g. router, switch, HUB, etc.), so that the devices become network facilities with RMON probe function. RMON NMS uses the basic SNMP commands to exchange data information with SNMP Agent and collect NM information. However, limited by the device resources, normally, not all the data of RMON MIB can be obtained with this method. In most cases, only four groups of information can be collected. The four groups include trap information, event information, history information and statistics information.

The Ethernet Switch implements RMON in the second method by far. With the RMON-supported SNMP Agent running on the network monitor, NMS can obtain such information as the overall traffic of the segment connected to the managed network device port, the error statistics and performance statistics, thereby implementing the management (generally remote management) over the network.

6.2 Configure RMON

RMON configuration includes:

- Add/Delete an Entry to/from the Alarm Table
- Add/Delete an Entry to/from the Event Table
- Add/Delete an Entry to/from the History Control Table
- Add/Delete an Entry to/from the extended RMON alarm table
- Add/Delete an Entry to/from the Statistics Table

6.2.1 Add/Delete an Entry to/from the Alarm Table

RMON alarm management can monitor the specified alarm variables such as the statistics on a port. When a value of the monitored data exceeds the defined threshold, an alarm event will be generated. Generally, the event will be recorded in the device log table and a Trap message will be sent to NMS. The events are defined in the event management. The alarm management includes browsing, adding and deleting the alarm entries.

You can use the following commands to add/delete an entry to/from the alarm table.

Perform the following configuration in system view.

Table 6-1 Add/Delete an entry to/from the alarm table

Operation	Command
Add an entry to the alarm table.	**rmon alarm** *entry-number alarm-variable sampling-time* { **delta** | **absolute** } **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* [**owner** *text*]
Delete an entry from the alarm table.	**undo rmon alarm** *entry-number*

6.2.2 Add/Delete an Entry to/from the Event Table

RMON event management defines the event ID and the handling of the event by keeping logs, sending Trap messages to NMS or performing the both at the same time.

You can use the following commands to add/delete an entry to/from the event table.

Perform the following configuration in system view.

Table 6-2 Add/Delete an entry to/from the event table

Operation	Command
Add an entry to the event table.	**rmon event** *event-entry* [**description** *string*] { **log** | **trap** *trap-community* | **log-trap** *log-trapcommunity* | **none** } [**owner** *rmon-station*]
Delete an entry from the event table.	**undo rmon event** *event-entry*

6.2.3 Add/Delete an Entry to/from the History Control Table

The history data management helps you set the history data collection, periodical data collection and storage of the specified ports. The sampling information includes the utilization ratio, error counts and total number of packets.

You can use the following commands to add/delete an entry to/from the history control table.

Perform the following configuration in Ethernet port view.

Table 6-3 Add/Delete an entry to/from the history control table

Operation	Command
Add an entry to the history control table.	**rmon history** *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *text-string*]
Delete an entry from the history control table.	**undo rmon history** *entry-number*

6.2.4 Add/Delete an Entry to/from the Extended RMON Alarm Table

You can use the command to add/delete an entry to/from the extended RMON alarm table.

Perform the following configuration in system view.

Table 6-4 Add/Delete an entry to/from the extended RMON alarm table

Operation	Command
Add an entry to the extended RMON alarm table.	**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]
Delete an entry from the extended RMON alarm table.	**undo rmon prialarm** *entry-number*

6.2.5 Add/Delete an Entry to/from the Statistics Table

The RMON statistics management concerns the port usage monitoring and error statistics when using the ports. The statistics include collision, CRC and queuing, undersize packets or oversize packets, timeout transmission, fragments, broadcast, multicast and unicast messages and the usage ratio of bandwidth.

You can use the following commands to add/delete an entry to/from the statistics table.

Perform the following configuration in Ethernet port view..

Table 6-5 Add/Delete an entry to/from the statistics table

Operation	Command
Add an entry to the statistics table	**rmon statistics** *entry-number* [**owner** *text-string*]
Delete an entry from the statistics table	**undo rmon statistics** *entry-number*

6.3 Display and Debug RMON

After the above configuration, execute **display** command in any view to display the running of the RMON configuration, and to verify the effect of the configuration.

Table 6-6 Display and debug RMON

Operation	Command
Display the RMON statistics	**display rmon statistics** [port-num]
Display the history information of RMON	**display rmon history** [*port-num*]
Display the alarm information of RMON	**display rmon alarm** [*alarm-table-entry*]
Display the extended alarm information of RMON	**display rmon prialarm** [*prialarm-table-entry*]
Display the RMON event	**display rmon event** [*event-table-entry*]
Display the event log of RMON	**display rmon eventlog** [*event-number*]

6.4 RMON Configuration Example

I. Networking requirements

Set an entry in RMON Ethernet statistics table for the Ethernet port performance, which is convenient for network administrators' query.

II. Networking diagram

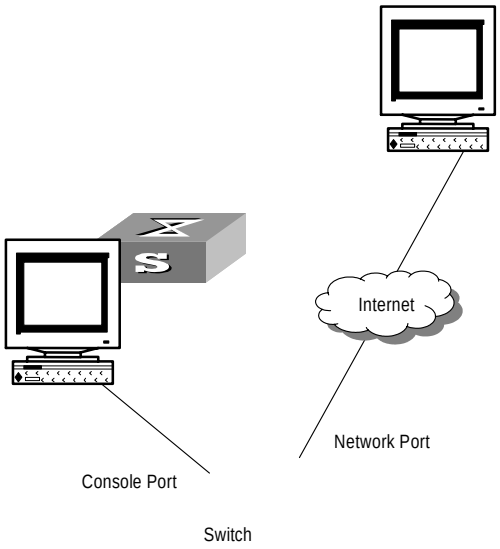


Figure 6-1 RMON configuration networking

III. Configuration procedure

Configure RMON.

```
[Quidway-Ethernet2/1] rmon statistics 1 owner huawei-rmon
```

View the configurations in user view.

```
<Quidway> display rmon statistics Ethernet 2/1
Statistics entry 1 owned by huawei-rmon is VALID.
  Gathers statistics of interface Ethernet2/1. Received:
  octets              : 270149,    packets          : 1954
  broadcast packets   :1570   ,    multicast packets:365
  undersized packets  :0      ,    oversized packets:0
  fragments packets   :0      ,    jabbers packets  :0
  CRC alignment errors:0      ,    collisions       :0
  Dropped packet events (due to lack of resources):0
  Packets received according to length (in octets):
  64     :644      ,  65-127  :518       ,  128-255  :688
  256-511:101      ,  512-1023:3         ,  1024-1518:0
```

Chapter 7 NTP Configuration

7.1 Brief Introduction to NTP

7.1.1 NTP Functions

As the network topology gets more and more complex, it becomes important to synchronize the clocks of the equipment on the whole network. NTP (Network Time Protocol) is an application layer protocol of TCP/IP and used for advertising the accurate time throughout the network.

NTP ensures the consistency of the following applications:

- For the increment backup between the backup server and client, NTP ensures the clock synchronization between the two systems.
- For multiple systems that coordinate to process a complex event, NTP ensures them to reference the same clock and guarantee the right order of the event.
- Guarantee the normal operation of the inter-system (Remote Procedure Call).
- Record for an application when a user logs in to a system, a file is modified, or some other operation is performed.

7.1.2 Basic Operating Principle of NTP

The following figure illustrates the basic operating principle of NTP:

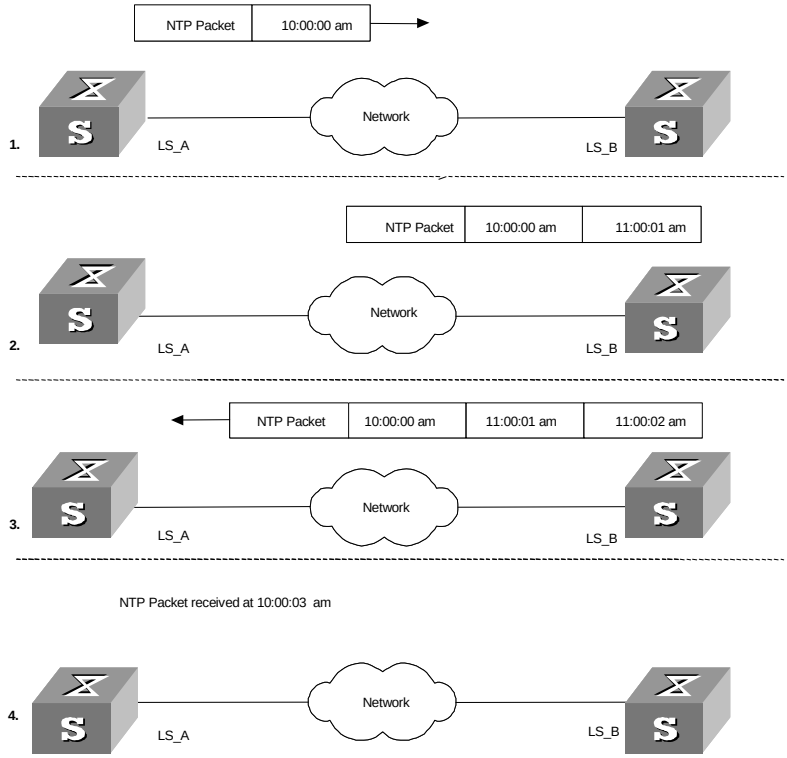


Figure 7-1 Basic operating principle of NTP

In the figure above, Ethernet Switch A and Ethernet Switch B are connected via the Ethernet port. They have independent system clocks. Before implement automatic clock synchronization on both switches, we assume that:

- Before synchronizing the system clocks on Ethernet Switch A and B, the clock on Ethernet Switch A is set to 10:00:00am, and that on B is set to 11:00:00am.
- Ethernet Switch B serves as an NTP time server. That is, Ethernet Switch A synchronizes the local clock with the clock of B.
- It takes 1 second to transmit a data packet from either A or B to the opposite end.

The system clocks are synchronized as follows:

- Ethernet Switch A sends an NTP packet to Ethernet Switch B. The packet carries the timestamp 10:00:00am (T_1) that tells when it left Ethernet Switch A.
- When the NTP packet arrives at Ethernet Switch B, Ethernet Switch B adds a local timestamp 11:00:01am (T_2) to it.
- When the NTP packet leaves Ethernet Switch B, Ethernet Switch B adds another local timestamp 11:00:02am (T_3) to it.
- When Ethernet Switch A receives the acknowledgement packet, it adds a new timestamp 10:00:03am (T_4) to it.

Now Ethernet Switch A collects enough information to calculate the following two important parameters:

- The delay for a round trip of an NTP packet traveling between the Switch A and B: Delay= $(T_4-T_1) - (T_3-T_2)$.
- Offset of Ethernet Switch A clock relative to Ethernet Switch B clock: offset= $((T_2-T_1) + (T_4-T_3)) /2$.

In this way, Ethernet Switch A uses the above information to set the local clock and synchronize it with the clock on Ethernet Switch B.

The operating principle of NTP is briefly introduced above. For details, refer to RFC1305.

7.2 NTP Configuration

NTP is used for time synchronization throughout a network. NTP configuration tasks include:

- Configure NTP operating mode
- Configure NTP ID authentication
- Set NTP authentication key
- Set the specified key to be reliable
- Set a local interface for transmitting NTP packets
- Set an external reference clock or the local clock as the master NTP clock
- Enable/Disable an interface to receive NTP packets
- Set control authority to access the local Ethernet Switch service.
- Set maximum local sessions
- Disable the NTP Service Globally

7.2.1 Configure NTP Operating Mode

You can set the NTP operating mode of an Ethernet Switch according to its location in the network and the network structure. For example, you can set a remote server as the time server of the local equipment. In this case the local Ethernet Switch works as an NTP client. If you set a remote server as a peer of the local Ethernet Switch, the local equipment operates in symmetric active mode. If you configure an interface on the local Ethernet Switch to transmit NTP broadcast packets, the local Ethernet Switch will operates in broadcast mode. If you configure an interface on the local Ethernet Switch to receive NTP broadcast packets, the local Ethernet Switch will operates in broadcast client mode. If you configure an interface on the local Ethernet Switch to transmit NTP multicast packets, the local Ethernet Switch will operates in multicast mode. Or you may also configure an interface on the local Ethernet Switch to receive NTP multicast packets, the local Ethernet Switch will operates in multicast client mode.

- Configure NTP server mode
- Configure NTP peer mode
- Configure NTP broadcast server mode
- Configure NTP broadcast client mode

- Configure NTP multicast server mode
- Configure NTP multicast client mode

I. Configure NTP Server Mode

Set a remote server whose ip address is *ip-address* as the local time server. *ip-address* specifies a host address other than a broadcast, multicast or reference clock IP address. In this case, the local Ethernet Switch operates in client mode. In this mode, only the local client synchronizes its clock with the clock of the remote server, while the reverse synchronization will not happen.

Perform the following configurations in system view.

Table 7-1 Configure NTP time server

Operation	Command
Configure NTP time server	**ntp-service unicast-server** *ip-address* [**version** *number*] [**authentication-keyid** *keyid*] [**source-interface** { *interface-name* | *interface-type interface-number* }] [**priority**]
Cancel NTP server mode	**undo ntp-service unicast-server** *ip-address*

NTP version number *number* ranges from 1 to 3 and defaults to 3; the authentication key ID *keyid* ranges from 0 to 4294967295; *interface-name* or *interface-type interface-number* specifies the IP address of an interface, from which the source IP address of the NTP packets sent from the local Ethernet Switch to the time server will be taken; **priority** indicates the time server will be the first choice.

II. Configure NTP Peer Mode

Set a remote server whose ip address is *ip-address* as the peer of the local equipment. In this case, the local equipment operates in symmetric active mode. *ip-address* specifies a host address other than a broadcast, multicast or reference clock IP address. In this mode, both the local Ethernet Switch and the remote server can synchronize their clocks with the clock of opposite end.

Perform the following configurations in system view.

Table 7-2 Configure NTP peer mode

Operation	Command
Configure NTP peer mode	**ntp-service unicast-peer** *ip-address* [**version** *number*] [**authentication-key** *keyid*] [**source-interface** { *interface-name* | *interface-type interface-number* }] [**priority**]
Cancel NTP peer mode	**undo ntp-service unicast-peer** *ip-address*

NTP version number *number* ranges from 1 to 3 and defaults to 3; the authentication key ID *keyid* ranges from 0 to 4294967295; *interface-name* or *interface-type interface-number* specifies the IP address of an interface, from which the source IP address of the NTP packets sent from the local Ethernet Switch to the peer will be taken; **priority** indicates the peer will be the first choice for time server.

III. Configure NTP Broadcast Server Mode

Designate an interface on the local Ethernet Switch to transmit NTP broadcast packets. In this case, the local equipment operates in broadcast mode and serves as a broadcast server to broadcast messages to its clients regularly.

Perform the following configurations in VLAN interface view.

Table 7-3 Configure NTP broadcast server mode

Operation	Command
Configure NTP broadcast server mode	**ntp-service broadcast-server** [**authentication-keyid** *keyid* **version** *number*]
Cancel NTP broadcast server mode	**undo ntp-service broadcast-server**

NTP version number *number* ranges from 1 to 3 and defaults to 3; the authentication key ID *keyid* ranges from 0 to 4294967295; This command can only be configured on the interface where the NTP broadcast packets will be transmitted.

IV. Configure NTP Broadcast Client Mode

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 packets, 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.

Perform the following configurations in VLAN interface view.

Table 7-4 Configure NTP broadcast client mode

Operation	Command
Configure NTP broadcast client mode	**ntp-service broadcast-client**
Disable NTP broadcast client mode	**undo ntp-service broadcast-client**

This command can only be configured on the interface where the NTP broadcast packets will be received.

V. Configure NTP Multicast Server Mode

Designate an interface on the local Ethernet Switch to transmit NTP multicast packets. In this case, the local equipment operates in multicast mode and serves as a multicast server to multicast messages to its clients regularly.

Perform the following configurations in VLAN interface view.

Table 7-5 Configure NTP multicast server mode

Operation	Command
Configure NTP multicast server mode	**ntp-service multicast-server** [*ip-address*] [**authentication-keyid** *keyid*] [**ttl** *ttl-number*] [**version** *number*]
Cancel NTP multicast server mode	**undo ntp-service multicast-server**

NTP version number *number* ranges from 1 to 3 and defaults to 3; the authentication key ID *keyid* ranges from 0 to 4294967295; *ttl-number* of the multicast packets ranges from 1 to 255; And the multicast IP address defaults to 224.0.1.1.

This command can only be configured on the interface where the NTP multicast packet will be transmitted.

VI. Configure NTP Multicast Client Mode

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 packets, 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 by the arrived multicast message.

Perform the following configurations in VLAN interface view.

Table 7-6 Configure NTP multicast client mode

Operation	Command
Configure NTP multicast client mode	**ntp-service multicast-client** [*ip-address*]
Cancel NTP multicast client mode	**undo ntp-service multicast-client**

Multicast IP address *ip-address* defaults to 224.0.1.1; This command can only be configured on the interface where the NTP multicast packets will be received.

7.2.2 Configure NTP ID Authentication

Enable NTP authentication, set MD5 authentication key, and specify the reliable key. A client will synchronize itself by a server only if the serve can provide a reliable key.

Perform the following configurations in system view.

Table 7-7 Configure NTP authentication

Operation	Command
Enable NTP authentication	**ntp-service authentication enable**
Disable NTP authentication	**undo ntp-service authentication enable**

7.2.3 Set NTP Authentication Key

This configuration task is to set NTP authentication key.

Perform the following configurations in system view.

Table 7-8 Configure NTP authentication key

Operation	Command
Configure NTP authentication key	**ntp-service authentication-keyid** *number* **authentication-mode md5** *value*
Remove NTP authentication key	**undo ntp-service authentication-keyid** *number*

Key number *number* ranges from 1 to 4294967295; the key *value* contains 1 to 32 ASCII characters.

7.2.4 Set Specified Key as Reliable

This configuration task is to set the specified key as reliable.

Perform the following configurations in system view.

Table 7-9 Set the specified key as reliable

Operation	Command
Set the specified key as reliable	**ntp-service reliable authentication-keyid** *key-number*
Cancel the specified reliable key.	**undo ntp-service reliable authentication-keyid** *key-number*

Key number *key-number* ranges from 1 to 4294967295

7.2.5 Designate an Interface to Transmit NTP Message

If the local equipment is configured to transmit all the NTP messages, these packets will have the same source IP address, which is taken from the IP address of the designated interface.

Perform the following configurations in system view.

Table 7-10 Designate an interface to transmit NTP message

Operation	Command
Designate an interface to transmit NTP message	**ntp-service source-interface** { *interface-name* | *interface-type interface-number* }
Cancel the interface to transmit NTP message	**undo ntp-service source-interface**

An interface is specified by *interface-name* or *interface-type interface-number*. The source address of the packets will be taken from the IP address of the interface. If the **ntp-service unicast-server** or **ntp-service unicast-peer** command also designates a transmitting interface, use the one designated by them.

7.2.6 Set NTP Master Clock

This configuration task is to set the external reference clock or the local clock as the NTP master clock.

Perform the following configurations in system view.

Table 7-11 Set the external reference clock or the local clock as the NTP master clock

Operation	Command
Set the external reference clock or the local clock as the NTP master clock.	**ntp-service refclock-master** [*ip-address*] [*stratum*]
Cancel the NTP master clock settings	**undo ntp-service refclock-master** [*ip-address*]

ip-address specifies the IP address 127.127.t.u of a reference clock, in which t ranges from 0 to 37 and u from 0 to 3. *stratum* specifies how many stratums the local clock belongs to and ranges from 1 to 15. If no IP address is specified, the system defaults to setting the local clock as the NTP master clock. You can specify the *stratum* parameter.

7.2.7 Enable/Disable an Interface to Receive NTP Message

This configuration task is to enable/disable an interface to receive NTP message.

Perform the following configurations in VLAN interface view.

Table 7-12 Enable/Disable an interface to receive NTP message

Operation	Command
Disable an interface to receive NTP message	**ntp-service in-interface disable**
Enable an interface to receive NTP message	**undo ntp-service in-interface disable**

This configuration task must be performed on the interface to be disabled to receive NTP message.

7.2.8 Set Authority to Access a Local Ethernet Switch

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**, **server**, **server only**, and **query only** in an ascending order of the limitation. The first matched authority will be given.

Perform the following configurations in system view.

Table 7-13 Set authority to access a local Ethernet switch

Operation	Command
Set authority to access a local Ethernet switch	**ntp-service access** { **query** | **synchronization** | **server** | **peer** } *acl-number*
Cancel settings of the authority to access a local Ethernet switch	**undo ntp-service access** { **query** | **synchronization** | **server** | **peer** }

IP address ACL number is specified through the *acl-number* parameter and ranges from 2000 to 2999. The meanings of other authority levels are as follows:

query: Allow control query for the local NTP service only.

synchronization: Allow request for local NTP time service only.

server: Allow local NTP time service request and control query. However, the local clock will not be synchronized by a remote server.

peer: Allow local NTP time service request and control query. And the local clock will also be synchronized by a remote server.

7.2.9 Set Maximum Local Sessions

This configuration task is to set the maximum local sessions.

Perform the following configurations in system view.

Table 7-14 Set the maximum local sessions

Operation	Command
Set the maximum local sessions	**ntp-service max-dynamic-sessions** *number*
Resume the maximum number of local sessions	**undo ntp-service max-dynamic-sessions**

number specifies the maximum number of local sessions, ranges from 0 to 100, and defaults to 100.

7.3 NTP Display and Debugging

After completing the above configurations, you can use the **display** command to show how NTP runs and verify the configurations according to the outputs.

In user view, you can use the **debugging** command to debug NTP.

Table 7-15 NTP display and debugging

Operation	Command
Display the status of NTP service	**display ntp-service status**
Display the status of sessions maintained by NTP service	**display ntp-service sessions** [**verbose**]
Display the brief information about every NTP time server on the way from the local equipment to the reference clock source.	**display ntp-service trace**
Enable NTP debugging	**debugging ntp-service**

7.4 Typical NTP Configuration Example

I. Configure NTP server

1) Network requirements

On Quidway1, set local clock as the NTP master clock at stratum 2. On Quidway2, configure Quidway1 as the time server in server mode and set the local equipment as in client mode.

2) Networking diagram

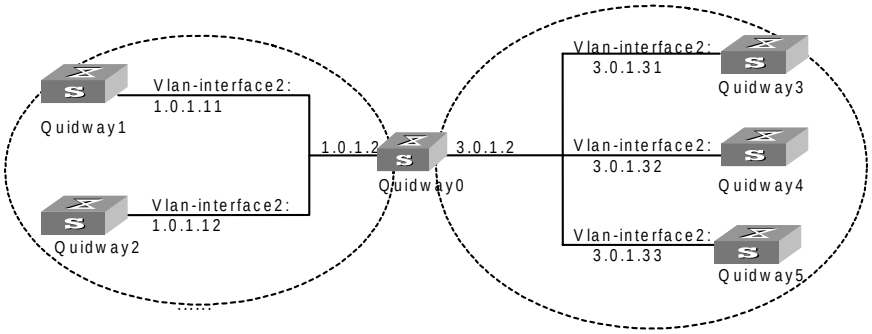


Figure 7-2 Typical NTP configuration networking diagram

3) Configuration procedure

Configure Ethernet Switch Quidway1:

Enter system view.

```
<Quidway1> system-view
```

Set the local clock as the NTP master clock at stratum 2.

```
[Quidway1] ntp-service refclock-master 2
```

Configure Ethernet Switch Quidway2:

Enter system view.

```
<Quidway2> system-view
```

Set Quidway1 as the NTP server.

```
[Quidway2] ntp-service unicast-server 1.0.1.11
```

The above examples synchronized Quidway2 by Quidway1. Before the synchronization, the Quidway2 is shown in the following status:

```
[Quidway2] 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)
```

After the synchronization, Quidway2 turns into the following status:

```
[Quidway2] display ntp-service status
Clock status: synchronized
```

```
Clock stratum: 3
Reference clock ID: 1.0.1.11
Nominal frequency: 60.0002 Hz
Actual frequency: 60.0002 Hz
Clock precision: 2^17
Clock offset: -9.8258 ms
Root delay: 27.10 ms
Root dispersion: 49.29 ms
Peer dispersion: 10.94 ms
Reference time: 19:21:32.287 UTC Oct 24 2004(C5267F3C.49A61E0C)
```

By this time, Quidway2 has been synchronized by Quidway1 and is at stratum 3, higher than Quidway1 by 1.

Display the sessions of Quidway2 and you will see Quidway2 has been connected with Quidway1.

```
[Quidway2] display ntp-service sessions
source            reference    stra reach poll  now offset  delay disper
**************************************************************************
[12345]1.0.1.11   LOCAL(0)     3    377   64   16   -0.4    0.0    0.9
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

II. NTP peer configuration example

1) Network requirements

On Quidway3, set local clock as the NTP master clock at stratum 2. On Quidway2, configure Quidway1 as the time server in server mode and set the local equipment as in client mode. At the same time, Quidway5 sets Quidway4 as its peer.

2) Networking diagram

See Figure 7-2.

3) Configuration procedure

Configure Ethernet Switch Quidway3:

Enter system view.

```
<Quidway3> system-view
```

Set the local clock as the NTP master clock at stratum 2.

```
[Quidway3] ntp-service refclock-master 2
```

Configure Ethernet Switch Quidway4:

Enter system view.

```
<Quidway4> system-view
```

Set Quidway1 as the NTP server at stratum 3 after synchronization.

```
[Quidway4] ntp-service unicast-server 3.0.1.31
```

Configure Ethernet Switch Quidway5: (Quidway4 has been synchronized by Quidway3)

Enter system view.

```
<Quidway5> system-view
```

Set the local clock as the NTP master clock at stratum 1.

```
[Quidway5] ntp-service refclock-master 1
```

After performing local synchronization, set Quidway4 as a peer.

```
[Quidway5] ntp-service unicast-peer 3.0.1.32
```

The above examples configure Quidway4 and Quidway5 as peers and configure Quidway5 as in active peer mode and Quidway4 in passive peer mode. Since Quidway5 is at stratum 1 and Quidway4 is at stratum 3, synchronize Quidway4 by Quidway5.

After synchronization, Quidway4 status is shown as follows:

```
[Quidway4] display ntp-service status
Clock status: synchronized
 Clock stratum: 2
 Reference clock ID: 3.0.1.31
 Nominal frequency: 60.0002 Hz
 Actual frequency: 60.0002 Hz
 Clock precision: 2^17
 Clock offset: -9.8258 ms
 Root delay: 27.10 ms
 Root dispersion: 49.29 ms
 Peer dispersion: 10.94 ms
 Reference time: 19:21:32.287 UTC Oct 24 2004(C5267F3C.49A61E0C)
```

By this time, Quidway4 has been synchronized by Quidway5 and it is at stratum 2, or higher than Quidway5 by 1.

Display the sessions of Quidway4 and you will see Quidway4 has been connected with Quidway5.

```
[Quidwa4] display ntp-service sessions
source            reference    stra reach poll  now offset  delay disper
**************************************************************
[12345]3.0.1.33   LOCAL(0)     2    377   64   16    0.0    0.0    0.9
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

III. Configure NTP broadcast mode

1) Network requirements

On Quidway3, set local clock as the NTP master clock at stratum 2 and configure to broadcast packets from Vlan-interface2. Configure Quidway4 and Quidway1 to listen to the broadcast from their Vlan-interface2 respectively.

2) Networking diagram

See Figure 7-2.

3) Configuration procedure

Configure Ethernet Switch Quidway3:

Enter system view.

```
<Quidway3> system-view
```

Set the local clock as the NTP master clock at stratum 2.

```
[Quidway3] ntp-service refclock-master 2
```

Enter Vlan-interface2 view.

```
[Quidway3] interface vlan-interface 2
```

Set it as broadcast server .

```
[Quidway3-Vlan-Interface2] ntp-service broadcast-server
```

Configure Ethernet Switch Quidway4:

Enter system view.

```
<Quidway4> system-view
```

Enter Vlan-interface2 view.

```
[Quidway4] interface vlan-interface 2
[Quidway4-Vlan-Interface2] ntp-service broadcast-client
```

Configure Ethernet Switch Quidway1:

Enter system view.

```
<Quidway1> system-view
```

Enter Vlan-interface2 view.

```
[Quidway1] interface vlan-interface 2
[Quidway1-Vlan-Interface2] ntp-service broadcast-client
```

The above examples configured Quidway4 and Quidway1 to listen to the broadcast via Vlan-interface2, Quidway3 to broadcast packets from Vlan-interface2. Since Quidway1 and Quidway3 are not located on the same segment, they cannot receive any broadcast packets from Quidway3, while Quidway4 is synchronized by Quidway3 after receiving its broadcast packet.

After the synchronization, you can find the state of Quidway4 as follows:

```
[Quidway4] display ntp-service status
clock status: synchronized
 clock stratum: 3
```

```
 reference clock ID: LOCAL(0)
 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: 10.94 ms
 peer dispersion: 10.00 ms
 reference time: 20:54:25.156 UTC Mar 7 2002(C0325201.2811A112)
```

By this time, Quidway4 has been synchronized by Quidway3 and it is at stratum 3, higher than Quidway3 by 1.

Display the status of Quidway4 sessions and you will see Quidway4 has been connected to Quidway3.

```
[Quidway2] display ntp-service sessions
  source              reference    stra reach poll  now offset  delay disper
[12345]127.127.1.0    LOCAL(0)     7   377    64   57   0.0    0.0    1.0
[5]1.0.1.11           LOCAL(0)     3    0     64    -    0.0    0.0    0.0
[5]128.108.22.44      0.0.0.0      16   0     64    -    0.0    0.0    0.0
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

IV. Configure NTP multicast mode

1) Network requirements

Quidway3 sets the local clock as the master clock at stratum 2 and multicast packets from Vlan-interface2. Set Quidway4 and Quidway1 to receive multicast messages from their respective Vlan-interface2.

2) Networking diagram

See Figure 7-2.

3) Configuration procedure

Configure Ethernet Switch Quidway3:

Enter system view.

```
<Quidway3> system-view
```

Set the local clock as a master NTP clock at stratum 2.

```
[Quidway3] ntp-service refclock-master 2
```

Enter Vlan-interface2 view.

```
[Quidway3] interface vlan-interface 2
```

Set it as a multicast server.

```
[Quidway3-Vlan-Interface2] ntp-service multicast-server
```

Configure Ethernet Switch Quidway4:

Enter system view.

```
<Quidway4> system-view
```

Enter Vlan-interface2 view.

```
[Quidway4] interface vlan-interface 2
```

Enable multicast client mode.

```
[Quidway4-Vlan-Interface2] ntp-service multicast-client
```

Configure Ethernet Switch Quidway1:

Enter system view.

```
<Quidway1> system-view
```

Enter Vlan-interface2 view.

```
[Quidway1] interface vlan-interface 2
```

Enable multicast client mode.

```
[Quidway1-Vlan-Interface2] ntp-service multicast-client
```

The above examples configure Quidway4 and Quidway1 to receive multicast messages from Vlan-interface2, Quidway3 multicast messages from Vlan-interface2. Since Quidway1 and Quidway3 are not located on the same segments, Quidway1 cannot receive the multicast packets from Quidway3, while Quidway4 is synchronized by Quidway3 after receiving the multicast packet.

V. Configure authentication-enabled NTP server mode

1) Network requirements

Quidway1 sets the local clock as the NTP master clock at stratum 2. Quidway2 sets Quidway1 as its time server in server mode and itself in client mode and enables authentication.

2) Networking diagram

See Figure 7-2.

3) Configuration procedure

Configure Ethernet Switch Quidway1:

Enter system view.

```
<Quidway1> system-view
```

Set the local clock as the master NTP clock at stratum 2.

```
[Quidway1] ntp-service refclcok-master 2
```

Configure Ethernet Switch Quidway2:

Enter system view.

```
<Quidway2> system-view
```

Set Quidway1 as time server.

```
[Quidway2] ntp-service unicast-server 1.0.1.11
```

Enable authentication.

```
[Quidway2] ntp-service authentication enable
```

Set the key.

```
[Quidway2] ntp-service authentication-keyid 42 authentication-mode md5
aNiceKey
```

Set the key as reliable.

```
[Quidway2] ntp-service reliable authentication-keyid 42
[Qudiway2] ntp-service unicast-server 1.0.1.11 authentication-keyid 42
```

The above examples synchronized Quidway2 by Quidway1. Since Quidway1 has not been enabled authentication, it cannot synchronize Quidway2. And now let us do the following additional configurations on Quidway1 :

Enable authentication.

```
[Quidway1] ntp-service authentication enable
```

Set the key.

```
[Quidway1] ntp-service authentication-keyid 42 authentication-mode md5
aNiceKey
```

Configure the key as reliable.

```
[Quidway1] ntp-service reliable authentication-keyid 42
```

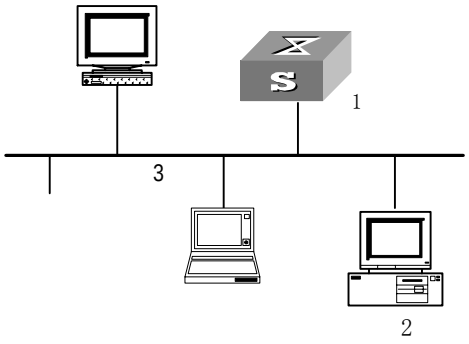
Chapter 8 SSH Terminal Services

8.1 SSH Terminal Services

8.1.1 SSH Overview

Secure Shell (SSH) can provide information security and powerful authentication to prevent such assaults as IP address spoofing, plain-text password interception when users log on to the switch remotely from an insecure network environment. A switch can connect to multiple SSH clients. SSH Client functions to enable SSH connections between users and the Ethernet switch or UNIX host that support SSH Server. You can set up SSH channels for local connection. See Figure 8-1.

Currently the switch which runs SSH server supports SSH version 1.5.



1: Switch running SSH server 2: PC running SSH client 3: Ethernet LAN

Figure 8-1 Setting up SSH channels in LAN

Note:

In the above figure, the VLAN for the Ethernet port must have been configured with VLAN interfaces and IP address.

The communication process between the server and client include these five stages: version negotiation stage, key negotiation stage, authentication stage, session request stage, interactive session stage.

- Version negotiation stage: The client sends TCP connection requirement to the server. When TCP connection is established, both ends begin to negotiate SSH version. If they can work together in harmony, they enter key algorithm negotiation stage. Otherwise the server clears the TCP connection.

- Key negotiation stage: Both ends negotiate key algorithm and compute session key. The server randomly generates its RSA key and sends the public key to the client. The client figures out session key based on the public key from the server and the random number generated locally. The client encrypts the random number with the public key from the server and sends the result back to the server. The server then decrypts the received data with the server private key to get the client random number. It then uses the same algorithm to work out the session key based on server public key and the returned random number. Then both ends get the same key without data transfer over the network, while the key is used at both ends for encryption and description.
- Authentication stage: The server authenticates the user at the client after obtaining session key. The client sends its username to the server: If the username has been created and configured as no authentication, authentication stage is skipped for this user. Otherwise, authentication process continues. SSH supports two authentication types: password authentication and RSA authentication. In the first type, the server compare the username and password received with those configured locally. The user is allowed to log on to the switch if the usernames and passwords match exactly. RSA authentication works in this way: The RSA public key of the client user is configured at the server. The client first sends the member modules of its RSA public key to the server, which checks its validity. If it is valid, the server generates a random number, which is sent to the client after being encrypted with RSA public key. Both ends calculate authentication data based on the random number and session ID. The client sends the authentication data calculated back to the server, which compares it with its attention data obtained locally. If they match exactly, the user is allowed to access the switch. Otherwise, authentication process fails.
- Session request stage: The client sends session request messages to the server which processes the request messages.
- Interactive session stage: Both ends exchange data till the session ends.

Session packets are encrypted in transfer and the session key is generated randomly. Encryption is used in exchanging session key and RSA authentication achieves key exchange without transfer over the network. SSH can protect server-client data security to the uttermost. The authentication will also start even if the username received is not configured at the server, so malicious intruders cannot judge whether a username they key in exists or not. This is also a way to protect username.

8.1.2 Configuring SSH Server

Basic configuration tasks refer to those required for successful connection from SSH client to SSH server, which advanced configuration tasks are those modifying SSH parameters.

Configuration tasks on SSH server include:

- Setting system protocol and link maximum
- Configuring and deleting local RSA key pair
- Configuring authentication type
- Defining update interval of server key
- Defining SSH authentication timeout value
- Defining SSH authentication retry value
- Entering public key view and editing public key
- Associating public key with SSH user

I. Setting system protocol

By default, the system only supports Telnet protocol, so you must specify SSH protocol for the system before enabling SSH.

Please perform the following configuration in system view.

Table 8-1 Setting system protocols and link maximum

Operation	Command
Set system protocol and link maximum	**protocol inbound** { **all** | **ssh** | **telnet** }

Caution:

If SSH protocol is specified, to ensure a successful login, 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**. When you configure SSH protocol successfully for the user interface, then you cannot configure **authentication-mode password** and **authentication-mode none** any more.

II. Configuring and canceling local RSA key pair

In executing this command, if you have configured RSA host key pair, the system gives an alarm after using this command and prompts that the existing one will be replaced. The server key pair is created dynamically by SSH server. The maximum bit range of both key pairs is 2048 bits and the minimum is 512.

Please perform the following configurations in system view.

Table 8-2 Configuring and canceling local RSA key pair

Operation	Command
Configure local RSA key pair	**rsa local-key-pair create**
Cancel local RSA key pair	**rsa local-key-pair destroy**

Caution:

For a successful SSH login, 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.

III. Configuring authentication type

For a new user, you must specify authentication type. Otherwise, he/she cannot access the switch.

Please perform the following configurations in system view.

Table 8-3 Configuring authentication type

Operation	Command
Configure authentication type	**ssh user** *username* **authentication-type** { **password** | **rsa** | **all** }
Remove authentication type setting	**undo ssh user** *username* **authentication-type**

If the configuration is RSA authentication type, then the RSA public key of client user must be configured on the switch, that is to perform the 7 and 8 serial number marked configuration.

By default, no authentication type is specified for a new user, so he/she cannot access the switch.

IV. Defining update interval of server key

Please perform the following configurations in system view.

Table 8-4 Defining update interval of server key

Operation	Command
Define update interval of server key	**ssh server rekey-interval** *hours*
Restore the default update interval	**undo ssh server rekey-interval**

By default, the system does not update server key.

V. Defining SSH authentication timeout value

Please perform the following configurations in system view.

Table 8-5 Defining SSH authentication timeout value

Operation	Command
Define SSH authentication timeout value	**ssh server timeout** *seconds*
Restore the default timeout value	**undo ssh server timeout**

By default, the timeout value for SSH authentication is 60 seconds.

VI. Defining SSH authentication retry value

Setting SSH authentication retry value can effectively prevent malicious registration attempt.

Please perform the following configurations in system view.

Table 8-6 Defining SSH authentication retry value

Operation	Command
Define SSH authentication retry value	**ssh server authentication-retries** *times*
Restore the default retry value	**undo ssh server authentication-retries**

By default, the retry value is 3.

VII. Entering public key edit view and editing public key

You can enter the public key edit view and edit the client public key.

Note:

This operation is only available for the SSH users using RSA authentication. At the switch, you configure the RSA public key of the client, while at the client, you specify the RSA private key which corresponds to the RSA public key.
This operation will fail if you configure password authentication for the SSH user.

Please perform the following configurations in system view.

Table 8-7 Configuring public key

Operation	Command
Enter public key view	**rsa peer-public-key** *key-name*
Delete a designated public key	**undo rsa peer-public-key** *key-name*

When entering the public key edit view with the **rsa peer-public-key** command, you can begin editing the public key with the **public-key-code begin** command. You can key in blank space between characters, since the system can remove the blank space automatically. But the public key should be composed of hexadecimal characters. Terminate public key editing and save the result with the **public-key-code end** command. Validity check comes before saving: the public key editing fails if the key contains invalid characters.

Please perform the following configurations in the public key view.

Table 8-8 Starting/terminating public key editing

Operation	Command
Enter public key edit view	**public-key-code begin**
Terminate public key edit view	**public-key-code end**
Quit public key view	**peer-public-key end**

VIII. Associating public key with SSH user

Please perform the following configurations in system view.

Table 8-9 Associating public key with SSH user

Operation	Command
Associate existing public with an SSH user	**ssh user** *username* **assign rsa-key** *keyname*
Remove the association	**undo ssh user** *username* **assign rsa-key**

8.1.3 Configuring SSH Client

There are several types of SSH client software, such as PuTTY and FreeBSD. You should first configure the client's connection with the server. The basic configuration tasks on client include:

- Specifying server IP address.
- Selecting SSH protocol. The client supports the remote connection protocols link Telnet, Rlogin and SSH. To set up SSH connection, you must select SSH protocol.

- Choosing SSH version. The switch currently supports SSH Server 1.5, so you have to choose 1.5 or earlier version.
- Specifying RSA private key file. If you specify RSA authentication for the SSH user, you must specify RSA private key file. The RSA key, which includes the public key and private key, are generated by the client software. The former is configured in the server (switch) and the latter is in the client.

The following description takes the PuTTY as an example.

I. Specifying server IP address

Start PuTTY program and the client configuration interface pops up.

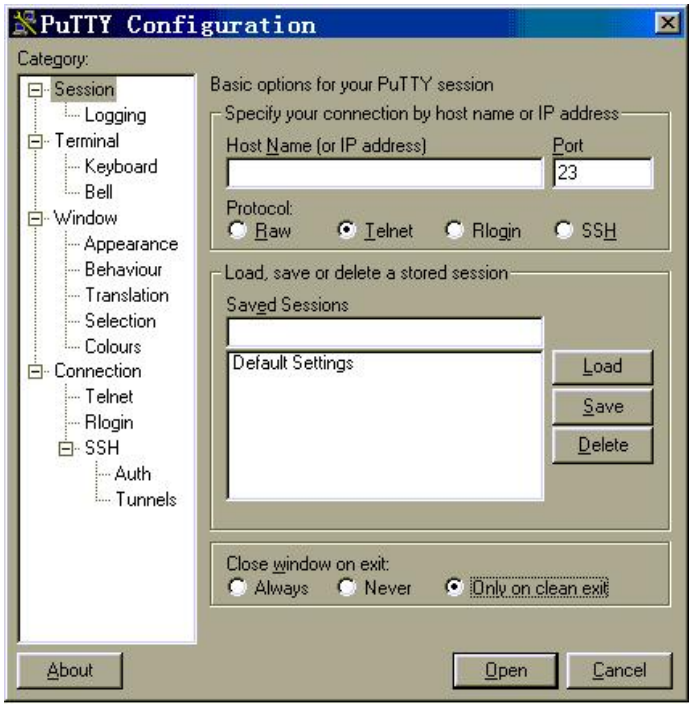


Figure 8-2 SSH client configuration interface (1)

In the Host Name (or IP address) text box key in the IP address of the switch, for example, 10.110.28.10. You can also input the IP address of an interface in UP state, but its route to SSH client PC must be reachable.

II. Selecting SSH protocol

Select SSH for the Protocol item.

III. Choosing SSH version

Click the left menu [Category/Connection/SSH] to enter the interface shown in following figure:

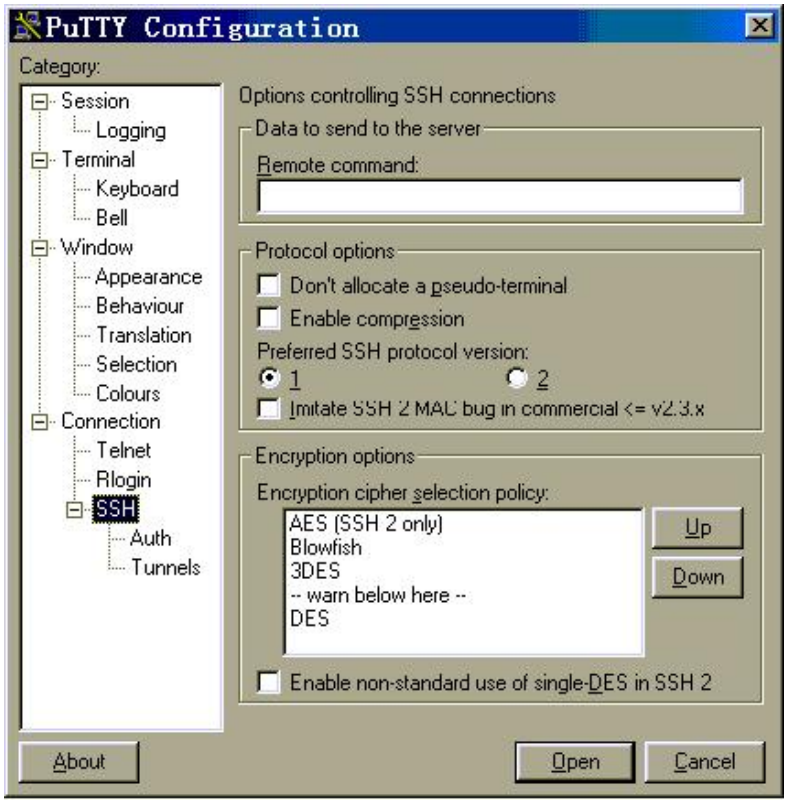


Figure 8-3 SSH client configuration interface (2)

You can select 1, as shown in the figure.

IV. Specifying RSA private key file

If you want to enable RSA authentication, you must specify RSA private key file, which is not required for password authentication.

Click [SSH/Auth] to enter the interface as shown in the following figure:

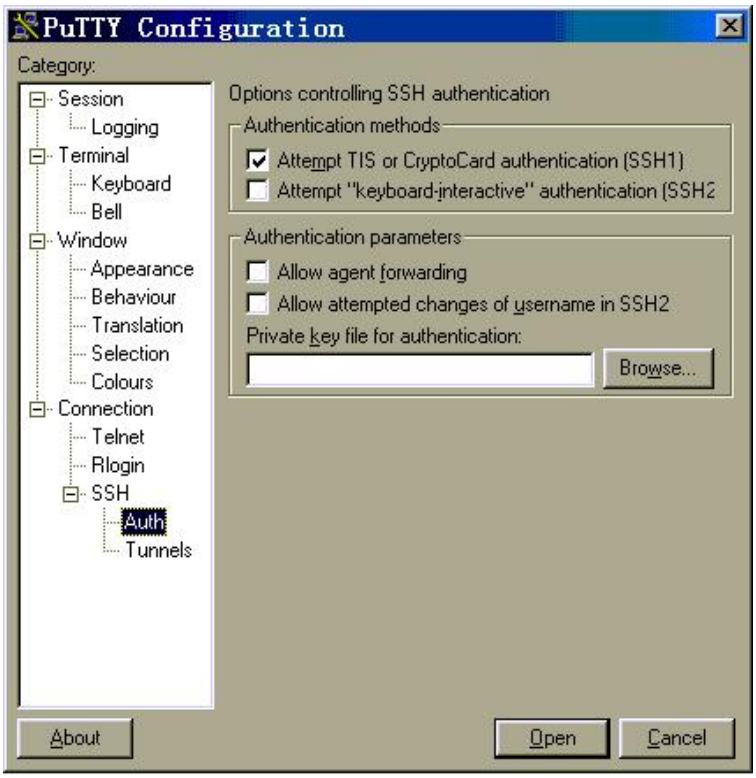


Figure 8-4 SSH client configuration interface (3)

Click the <Browse> button to enter the File Select interface. Choose a desired file and click <OK>.

V. Opening SSH connection

Click the <Open > button to enter SSH client interface. If it runs normally, you are promoted to enter username and password. See the following figure.

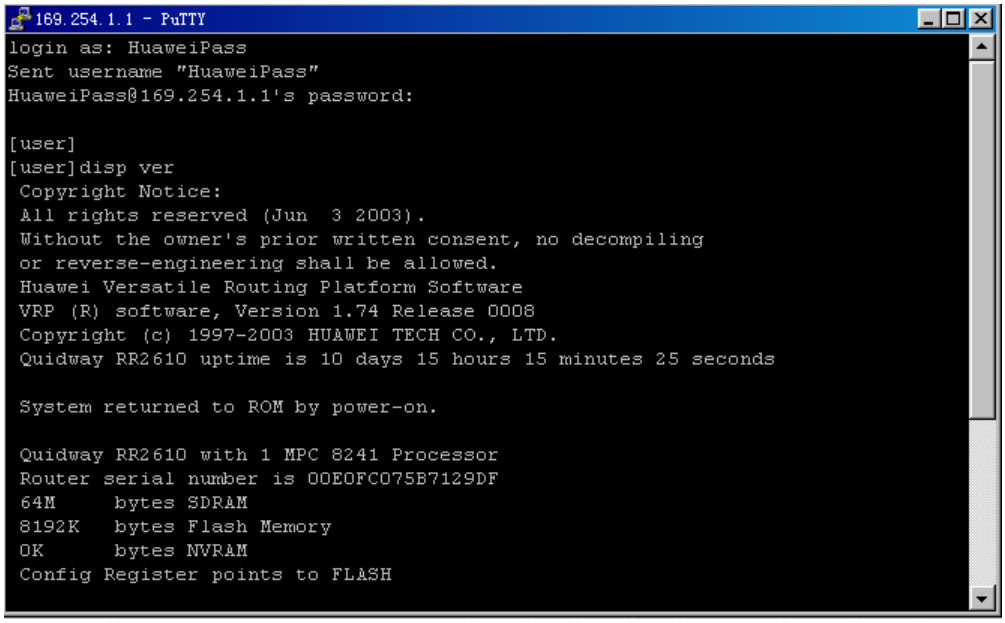


Figure 8-5 SSH client interface

1) Key in correct username and password and log into SSH connection.
2) Log out of SSH connection with the **logout** command.

8.1.4 Displaying and Debugging SSH

Run the **display** command in any view to view the running of SSH and further to check configuration result.

Run the **debugging** command to debug the SSH.

Please perform the following configurations in any view.

Table 8-10 Display SSH information

Operation	Command
Display host and server public keys	**display rsa local-key-pair public**
Display client RSA public key	**display rsa peer-public-key** [**brief** | **name** *keyname*]
Display SSH state information and session	**display ssh server** { **status** | **session** }
Display SSH user information	**display ssh user-information** [*username*]
Enable SSH debugging	**debugging ssh server** { **VTY** *index* | **all** }
Enable RSA debugging	**debugging rsa**
Disable SSH debugging	**undo debugging ssh server** { **VTY** *index* | **all** }
Disable RSA debugging	**undo debugging rsa**

8.1.5 SSH Configuration Example

I. Networking requirements

As shown in Figure 8-6, configure local connection from SSH Client to the switch. The client uses SSH protocol to access the switch.

II. Networking diagram

Figure 8-6 Networking for SSH local configuration

III. Configuration procedure

You should run this command before any other configuration:

```
[Quidway] rsa local-key-pair create
```

Note:

If you have configured local key pair in advance, this operation is unnecessary.

- For password authentication mode

```
[Quidway] user-interface vty 0 4
[Quidway-ui-vty0-4] authentication-mode scheme
[Quidway-ui-vty0-4] protocol inbound ssh
[Quidway] local-user client001
[Quidway-luser-client001] password simple huawei
[Quidway-luser-client001] service-type ssh
[Quidway] ssh user client001 authentication-type password
```

Select the default values for SSH authentication timeout value, retry value and update interval of server key. Then run SSH1.5 client program on the PC which is connected to the switch and access the switch using username “client001” and password “huawei”.

- For RSA authentication mode

Create local user client002

```
[Quidway] local-user client002
[Quidway-luser-client002] service-type ssh
```

Specify AAA authentication on the user interface.

```
[Quidway] user-interface vty 0 4
```

```
[Quidway-ui-vty0-4] authentication-mode scheme
```

Select SSH protocol on the switch.

```
[Quidway-ui-vty0-4] protocol inbound ssh
```

Specify RSA authentication on the switch.

```
[Quidway] ssh user client002 authentication-type RSA
```

Configure RSA key pair on the switch.

```
[Quidway] rsa peer-public-key quidway002
[Quidway-rsa-public] public-key-code begin
[Quidway-key-code] 308186028180739A291ABDA704F5D93DC8FDF84C427463
[Quidway-key-code] 1991C164B0DF178C55FA833591C7D47D5381D09CE82913
[Quidway-key-code] D7EDF9C08511D83CA4ED2B30B809808EB0D1F52D045DE4
[Quidway-key-code] 0861B74A0E135523CCD74CAC61F8E58C452B2F3F2DA0DC
[Quidway-key-code] C48E3306367FE187BDD944018B3B69F3CBB0A573202C16
[Quidway-key-code] BB2FC1ACF3EC8F828D55A36F1CDDC4BB45504F020125
[Quidway-key-code] public-key-code end
[Quidway-rsa-public] peer-public-key end
[Quidway] ssh user client002 assign rsa-key key002
```

Note:

You need to specify RSA private key which corresponds to the public key for the SSH user client002.

Run SSH1.5 client program on the PC which has been configured with private RSA private key and you can set up SSH connection.

HUAWEI

Quidway S3000-EI Series Ethernet Switches
Operation Manual

Remote Power-feeding

Table of Contents

Chapter 1 Remote Power-Feeding Configuration

1.1 Overview

S3026C-PWR Ethernet Switch provides Power over Ethernet (PoE) function, which performs remote power-feeding to connected powered devices (PD) such as IP phones, WLAN APs and Network cameras, by providing -48V DC power to the attached remote PDs through twisted-pairs.

- As a kind of power sourcing equipment (PSE), S3026C-PWR complies with the IEEE802.3af standard. Besides, it can also supply power to non-802.3af-compliant PDs.
- S3026C-PWR is capable of concurrent data transfer and current transfer through the signal lines 1, 3, 2 and 6 in category-3/category-5 twisted pairs. Alternatively, it can also use the signal lines 1, 3, 2 and 6 in category-3/category-5 twisted pairs to transfer data and use the spare lines 4, 5, 7 and 8 to transfer current. You can opt for either power supply mode by inputting command lines or pressing the mode button.
- S3026C-PWR supplies power to outside with 24 fixed Ethernet electrical ports. It can feed power to up to 24 remotely attached Ethernet switches, traveling a longest distance of 100m.
- Each Ethernet port can provide a maximum power of 15.4W to the devices connected to it.
- An S3026C-PWR as a whole provides a total of 160W at most during remote power-feeding. It decides whether to feed power to a next remote device according to the currently available power.

Note:

- If a remote PD receives power from an S3026C-PWR, it does not have to equip itself with any external power.
- If a remote PD does install an external power, the S3026C-PWR will work in conjunction with it to provide power redundancy backup to the PD.

1.2 Configuring Remote Power-Feeding

An S3026C-PWR can automatically checks up whether a connected device needs a remote power-feeding and supply power to those in demand.

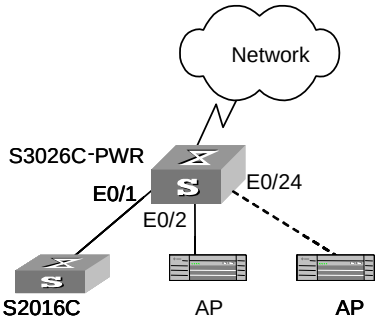


Figure 1-1 Remote power-feeding

You can input command lines to enable/disable remote power-feeding on a port, adjust its power-feeding mode and PD detection mode, and set its power-feeding priority and compatibility testing functionality. As such, you can also press the "mode" button to perform reverse detection on the PDs connected to an S3026C-PWR and allow the S3026C-PWR to supply power to PDs on spare lines and signal lines simultaneously.

Table 1-1 Configuring remote power-feeding

Device	Configuration	Default	Description
S3026C-PWR	Enable remote power-feeding on a port	Enabled	-
	Press the mode button to detect power-feeding on a port	-	-
	Select the power-feeding mode on a port	Power-feeding through signal lines	You can adjust the power-feeding mode if necessary.
	Set the maximum power on an power-feeding port	15400 milliwatt	You can adjust this maximum according to the power on the PDs in practice.
	Setting power management mode and Power-Feeding Priority on a Port	power management mode is manual mode Priority of a Port is Low	-
	Enable/Disable the compatibility detection on a port	Disabled	-
	Reset the PoE configuration on the switch	-	You can restore default PoE configuration on the current switch.
	Upgrading the PoE Daughter-Card	-	-

Device	Configuration	Default	Description
PD	Correctly connect the PD with the electrical ports of S3026C-PWR	-	-

1.2.1 Enabling/Disabling Remote Power-Feeding on a Port

You can enable or disable remote power-feeding on a port according to actual network requirements.

Perform the following configurations in Ethernet port view.

Table 1-2 Enabling/disabling remote power-feeding on a port

Operation	Command
Enable remote power-feeding on a port	**undo poe disable**
Disable remote power-feeding on a port	**poe disable**

By default, remote power-feeding is enabled on a port.

1.2.2 Pressing the Mode Button to Detect Power-Feeding on a Port

By default, S3026C-PWR feeds power to its connected PDs through signal lines. However, some PDs are actually powered via spare lines. Therefore, you can press the "mode" button on the front panel of S3026C-PWR to perform reverse detection on the connected PDs so as to find the "some" and feed power to them. The detection itself does not impact the ongoing power-feeding ports, for it only detects those ports that are not in service. Once it finds any PDs connected on certain ports are powered via spare lines, the system will supply power to them. The left LED of a port indicates the port power-feeding status: ON means the port is in service; OFF means the port is not in service; flashing means the port operates abnormally. The detection stops in 45 seconds. And then the ports not in service restore to signal lines mode.

1.2.3 Selecting the Power-Feeding Mode on a Port

S3026C-PWR is capable of concurrent data transfer and current transfer through the signal lines 1, 3, 2 and 6 in category-3/category-5 twisted pairs. Alternatively, it can also use the signal lines 1, 3, 2 and 6 in category-3/category-5 twisted pairs to transfer data and use the spare lines 4, 5, 7 and 8 to transfer current. You can opt for either power supply mode by inputting command lines or pressing the mode button.

You can select the power-feeding mode of a current port by executing the following commands.

Perform the following configurations in Ethernet port view.

Table 1-3 Selecting the power-feeding mode on a port

Operation	Command
Feed power through signal lines	**poe mode signal**
Feed power through spare lines	**poe mode spare**
Restore the default power-feeding mode	**undo poe mode**

By default, a port feeds power through signal lines.

1.2.4 Setting the Maximum Power on a Power-Feeding Port

Each Ethernet port of an S3026C-PWR can provide a maximum of 15400 milliwatt to the PDs connected to it. You can adjust this maximum between 0 and 15400 milliwatt according to the actual power of the PDs.

You can set the maximum power on an ongoing power-feeding port by executing the following commands.

Perform the following configurations in Ethernet port view.

Table 1-4 Setting the maximum power on a power-feeding port

Operation	Command
Set the maximum power on an power-feeding port	**poe max-power** *max-power*
Restore the default value	**undo poe max-power**

By default, a port supplies power under a maximum of 15400 milliwatt.

1.2.5 Setting power management mode and Power-Feeding Priority on a Port

An S3026C-PWR as a whole externally provides a total of 160W in extreme. By default, when reaching this maximum, the S3026C-PWR will not supply any power to any newly connected PDs.

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.

I. Setting power management mode

Perform the following configurations in system view to the power management mode.

Table 1-5 Setting power management mode

Operation	Command
Set the power management mode to auto mode	**poe power-management auto**
Set the power management mode to manual mode	**poe power-management manual**
Restore the default value	**undo poe power-management**

By default, the power management mode is manual mode.

II. Setting Power-Feeding Priority on a Port

Perform the following configurations in Ethernet port view to configure the power supply priority of the current port.

Table 1-6 Setting power-feeding priority on a port

Operation	Command
Set the power-feeding priority of a port	**poe priority** { **critical** | **high** | **low** }
Restore the default value	**undo poe priority**

By default, the power-feeding priority of a port is "low".

1.2.6 Enabling/Disabling the Compatibility Detection of 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 function reduces PD detection rate and the performance of the switch. You are recommended to disable this function when the PD devices are the ones complying 802.3af standard.

You can enable/disable the compatibility detection of PDs by executing the following commands.

Perform the following configurations in system view.

Table 1-7 Enabling/disabling the compatibility detection of PDs

Operation	Command
Enable the compatibility detection of PDs	**undo poe legacy disable**
Disable the compatibility detection of PDs	**poe legacy disable**

By default, the compatibility detection of PDs is enabled.

1.2.7 Reset the PoE Configuration on the Switch

You can use the following command to restore the default PoE configuration on the switch.

Perform the following configuration in user view.

Table 1-8 Reset the PoE Configuration on the Switch

Operation	Command
Reset the PoE configuration on the switch	reset poe-configuration

1.2.8 Upgrading the 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 process includes two steps:

1) Download the software of PoE daughter-card to switch Flash.
2) Upgrade the PoE daughter-card by command

User can use FTP, TFTP function of switch to download the software of PoE daughter-card to switch Flash. Detailed description reference to FTP and TFTP segment in “System Management” module of the Operation Manual. Here introduce step 2.

Perform the following configurations in system view to upgrade the PoE daughter-card.

Table 1-9 Upgrading the PoE daughter-card by Command

Operation	Command
Upgrading the PoE daughter-card by Command	**poe update** *file-url*

The extent name of the application file should be “bin”.

1.3 Displaying Remote Power-Feeding

After the above configuration, execute the **display** commands in any view to display the running of the remote power-feeding configuration, and to verify the effect of the configuration.

Table 1-10 Displaying remote power-feeding

Operation	Command
Display the remote power-feeding status of specified port or all ports	**display poe interface** { *interface-name* | *interface-type interface-num* | **all** }
Display the power of specified port or all ports	**display poe interface power** { *interface-name* | *interface-type interface-num* | **all** }
Display the PoE parameters of PSE power supply device	**display poe powersupply**

For details about the parameters, refer to the relevant command manual.

1.4 Configuration Example

1.4.1 Power-feeding Supply Configuration Example

I. Networking requirements

Ethernet0/1 of the S3026C-PWR connects to an S2016C Ethernet switch, Ethernet0/2 connects to an Access Point (AP) and Ethernet0/24 is supposed to connect to an important AP.

The S3026C-PWR supply power to its connected devices, including those non-802.3af-compliant PDs. Among the ports, Ethernet0/2 supply power to outside through spare lines. The AP devices have a power consumption of 2500 milliwatt and S2016C 12000 milliwatt. Even if the S3026C-PWR supplies power to the full, PDs connected to Ethernet0/24 shall be powered preferentially.

II. Networking diagram

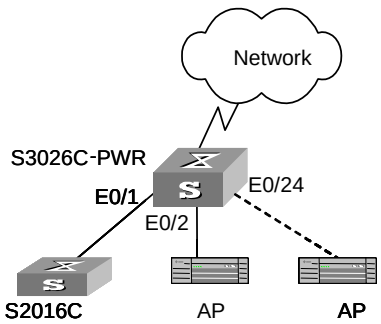


Figure 1-2 An example for remote power-feeding

III. Configuration procedure

Enable remote power-feeding on Ethernet0/1, Ethernet0/2 and Ethernet0/24 (this is the default configuration and can be therefore omitted.)

```
[Quidway-Ethernet0/1] undo poe disable
[Quidway-Ethernet0/2] undo poe disable
[Quidway-Ethernet0/24] undo poe disable
```

Enable Ethernet0/2 to supply power through spare lines.

```
[Quidway-Ethernet0/2] poe mode spare
```

Set Ethernet0/1 to have a maximum power of 12000 milliwatt and Ethernet0/2 3000 milliwatt.

```
[Quidway-Ethernet0/1] poe max-power 12000
[Quidway-Ethernet0/2] poe max-power 3000
```

Set the priority of Ethernet0/24 to be critical to ensure preferential power supply for its PDs.

```
[Quidway-Ethernet0/24] poe priority critical
```

Configure the power management mode in auto mode.

```
[Quidway] poe power-management auto
```

Enable the compatibility detection of PDs on the switch so that it can supply power to those PDs that do not comply with 802.3af.

```
[Quidway] undo poe legacy disable
```

1.4.2 Upgrading PoE daughter-card Configuration Example

I. Networking requirements

The switch serves as FTP client and the remote PC as FTP server. The configuration on FTP server: Configure a FTP user named as switch, with password hello and with read & write authority over the Switch root directory on the PC. The IP address of a VLAN interface on the switch is 1.1.1.1, and that of the PC is 2.2.2.2. The switch and PC are reachable.

The PoE daughter-card application file new.bin is stored on the PC. Using FTP, the switch can download the new.bin from the remote FTP server and then upgrade the PoE daughter-card .

II. Networking diagram

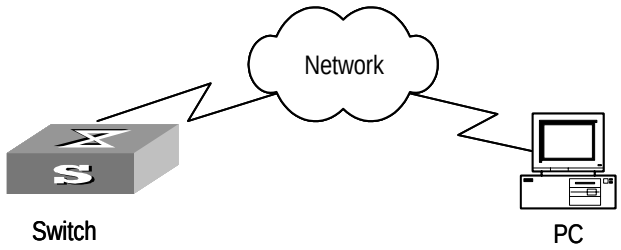


Figure 1-3 Networking for FTP configuration

III. Configuration procedure

1) Configure FTP server parameters on the PC: a user named as switch, password hello, read & write authority over the Switch directory on the PC.
2) Configure the switch

Log into the switch (locally through the Console port or remotely using Telnet).

```
<Quidway>
```

Caution:

If the flash memory of the switch is not enough, you need to first delete the existing programs in the flash memory and then upload the new ones.

Type in the right command in user view to establish FTP connection, then correct username and password to log into the FTP server.

```
<Quidway> ftp 2.2.2.2
Trying ...
Press CTRL+K to abort
Connected.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(none):switch
331 Give me your password, please
Password:*****
230 Logged in successfully
[ftp]
```

Type in the authorized directory of the FTP server.

```
[ftp] cd switch
```

Use the **get** command to download the new.bin from the FTP server to the flash directory on the FTP server.

```
[ftp] get new.bin
```

Use the **quit** command to release FTP connection and return to user view.

```
[ftp] quit
<Quidway>
```

Enter system view.

```
<Quidway> system-view
[Quidway]
```

Use the **poe update** command to upgrade the PoE daughter-card.

```
[Quidway] poe update flash:/new.bin
```

HUAWEI

Quidway S3000-EI Series Ethernet Switches
Operation Manual

Appendix

Table of Contents

Appendix A Acronyms

A	
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
ARP	Address Resolution Protocol
C	
CLI	Command Line Interface
F	
FTP	File Transfer Protocol
G	
GARP	Generic Attribute Registration Protocol
GE	Gigabit Ethernet
GVRP	GARP VLAN Registration Protocol
GMRP	GARP Multicast Registration Protocol
H	
HGMP	Huawei Group Management Protocol
I	
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP	Internet Protocol
M	
MAC	Medium Access Control
MIB	Management Information Base
N	
NMS	Network Management System
NVRAM	Nonvolatile RAM
Q	
QoS	Quality of Service
R	
RMON	Remote Network Monitoring
RSTP	Rapid Spanning Tree Protocol

S	
SNMP	Simple Network Management Protocol
STP	Spanning Tree Protocol
T	
TCP/IP	Transmission Control Protocol/ Internet Protocol
TFTP	Trivial File Transfer Protocol
TTL	Time To Live
U	
UDP	User Datagram Protocol
V	
VLAN	Virtual LAN
VOD	Video On Demand
VT	Virtual Terminal
VTY	Virtual Type Terminal