Layer-2 Ethernet Switch

QSW-2870

Preface

Manual Instruction

This manual introduces the QSW-2870 Series Carrier Class Layer-2 Full-Giga Ethernet Switch telecommunication level (hereinafter referred to as the QSW-2870) of various functional modules and service operation guidelines based on CLI, including the basic configuration, the two layers configuration operation of the QSW-2870, IP service, QoS configuration, multicasting, security, reliability, device Management and network Management etc. The above operation are introduced from the simple principle, function configuration step and configuration example in three ways. The configuration operation helps user to master the configuration method of QSW-2870 and understand its application scenarios, more specialized professional to use, maintenance and management of QSW-2870

Intended Audience

The manual is intended for the following readers:

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

Content Introduction

Chapter	Summary
Chapter1 Basic Configuration	To introduce basic configuration to QSW-2870 Switch;
Chapter2 Layer 2 Ethernet Configuration	To introduce Layer2 Ethernet configuration QSW-2870 Switch;
Chapter3 IP Service Configuration	To introduce IP configuration;
Chapter4 Routing Configuration	To introduce route information of QSW-2870 Switch;
Chapter5 QoS Configuration	To introduce QSW-2870 switch QoS configuration;
Chapter6 IGMP Configuration	To introduce IGMP configuration;
Chapter7 Security Configuration	To introduce security configuration;

Chapter	Summary
Chapter8 Reliability Configuration	To introduce reliability facilities of QSW-2870 Switch;
Chapter9 PoE Configuration	To introduce configuration of PoE functionalities of QSW-2870 Switch;

Release Update Instruction

Software Version	Manual Release	Update Description
	V1.0	First publishment

Manual Convention

Introduce general format, symbol convention, keyboard/mouse operation and safety signs.

2. General Format

Typeface	Description
Arial	Standard font for manual text including Arabic numerals
Bold	Chapter/Section names menus, menu options, radio button names, check boxes, drop-down lists, dialog box names, window names.

3. Symbol Convention

Typeface	Description
< >	Keyboard typing names, button names, input contents from a certain terminal.
[ ]	Optional parameters, menu bars, datasheets, fragments/octets.
→	Separator of multi-menus/paths, e.g., “Main menu → Sub-menu → Root menu”

4. Keyboard Operation Convention

Typeface	Description

Typeface	Description
Characters with angle brackets	Indicates Keyboard typing names or button names, e.g. ＜Enter＞, ＜Tab＞, ＜Backspace＞, ＜a＞are respectively indicating keyboard enter, tab, backspace and lowercase character “a”.
＜Keyboard 1+Keyboard 2＞	Indicates press 2 or more keys at the same time, e.g.,＜Ctrl+Alt+A＞ indicates to press “Ctrl”、“Alt”、“A” at the same time.
＜Keyboard 1, Keyboard 2＞	Indicates press key 1 first, release and then press key 2., e.g.,＜Alt, F＞ indicates to press “Alt” first , then release and finally press “F”.

5. Mouse Operation Convention

Typeface	Description
Click	Refers to clicking primary mouse button (usually left mouse button) once
Double-click	Refers to quick clicking primary mouse button (usually left mouse button) twice
Right-click	Refers to clicking secondary mouse button (usually right mouse button) once
Drag	Refers to pressing and holding a mouse button and moving mouse

6. Safety Signs

This manual utilizes general 3 safety signs to emphasis significances during operation, installation or maintenance.

 **Notice**,  **Attention**,  **Warning**

Legal Disclaimer

Qtech Co., commits itself to ensure accuracy, fidelity and reliability to the manual contents, however does not take any legal responsibility of any loss or damage caused by possible pretermission, inaccuracy or error in this manual.

Table of Contents

Figure

Chapter1
Basic Configuration

1.1 Summary

This chapter generally introduces fundamental configuration and operation to QSW-2870 switch.

This chapter includes the following section.

1.2 Interface Introduction

QSW-2870 interface is the unit which provides to the user operation or configuration; it is mainly used for sending and receiving data.

Functionally, the interface can be divided into Management interface and service interface.

1.2.1 Management Interface

Background Information

The management interface is classified for distinguishing from service interface. It provides supports for users on configuration and management manner, that through which the user is able to login the QSW-2870 Switch and process configurable and manageable operations. The management interface does not undertake service and data transmission.

Process

The QSW-2870 Switch provides two types of management interface, CONSOLE port and ETH port.

Interface Name	Interface Description	Interface Application

Console port	comply with EIA/TIA-232 Standard with interface type DCE	connected with COM serial port of configuration terminal for building local configuration environment
ETH port	comply with 10/100BASE-TX Standard	connected with network port of configuration terminal or NM station, for building local or remote configuration environment

1.2.2 Physical Interface

Background Information

Physical interface indicates ones that physically exist. The physical interfaces of QSW-2870 Switch are deployed at switching main control board and PCB board.

The physical interfaces include management ports and service ports.

Process

The QSW-2870 Switch is supporting physical interfaces including:

- Console Port
- ETH Port
- Fast Ethernet (FE) Port

1.3 Login Switch

1.3.1 Login through Console Port

Purpose

This section introduces how to login QSW-2870 Switch through Console port of local PC.

Precondition

Before the login of QSW-2870 Switch via hyper terminal, the user shall confirm the following issue:

- The QSW-2870 Switch has been OS and FPGA versions uploaded.

Requirement

When logging into QSW-2870 Switch through Console port, the user needs to connect to the Console port of QSW-2870 front panel with a serial line.

Process

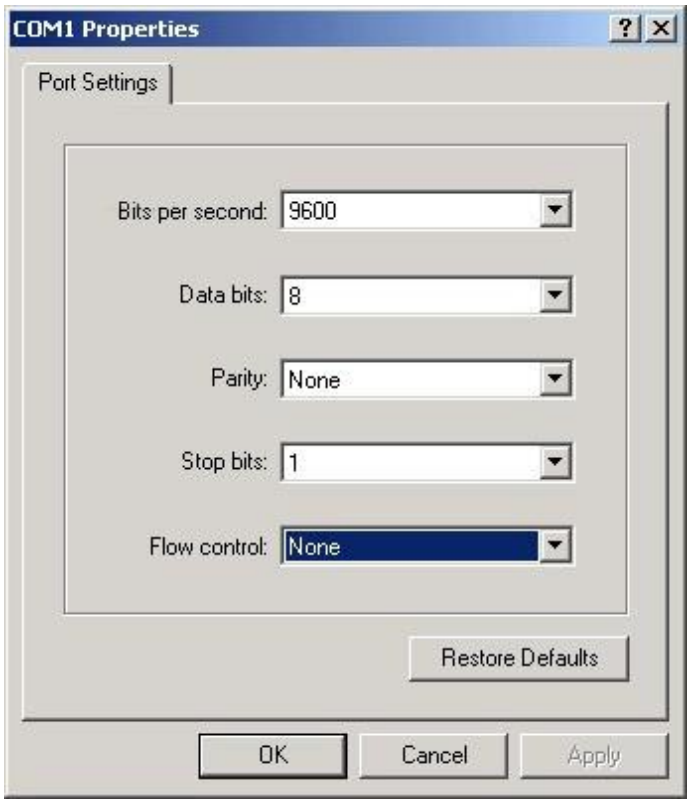
The processes of logging into QSW-2870 Switch through Console port are as follows:

- Connect the PC host and QSW-2870 Switch via a serial line, referring to Figure 1-1 QSW-2870 Switch Login through Console Port;
- Start PC hyper terminal by selecting [Start → All Programs → Accessories → Communication], there will be a pop-up window of connection description;
- Create a new connection:

  Input a name to the new created connection in the [Name] column, e.g.,QSW-2870

- Connection port setting. Select COM1 or COM2 port according to physical connection of serial line, and click <OK>

- Serial port setting. Please perform the settings according to Serial Port Property Setting of QSW-2870 Switch:



Serial Port Property Setting of QSW-2870 Switch

Please set the parameters according to table shown in Table 1-1 Parameter Description when Logging QSW-2870 Switch through Serial Line:

Table 1-1 Parameter Description when Logging QSW-2870 Switch through Serial Line

Parameter	Value
Bit per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

- Click <OK> to confirm.

Result

If settings are performed according to above processes and the device is in normal operation, there will be hyper terminal interface displayed Login Interface of Hyper Terminal indicating the hyper terminal has been successfully logging into the QSW-2870 Switch.

1.3.2 Login through Telnet

Purpose

Besides hyper terminal, the login of QSW-2870 Switch can also be achieved through telnet. The serial port provided by the QSW-2870 Switch offers regular version upload, upgrade and maintenance only.

The section introduces how to use local PC to log into QSW-2870 Switch through telnet. Local PC telnet supports local and remote user login which is easy for maintenance.

Precondition

Before the login of QSW-2870 Switch via telnet, the user shall confirm the following issue:

- The QSW-2870 Switch is „ping" available with local PC.

Network Requirement

When logging to QSW-2870 Switch via telnet, there shall be direct network cable connection or connection with hub.
Once the telnet is utilized for login, the QSW-2870 Switch must be configured as telnet user with username and password.

Process

The processes of telnet login are as follows:

1. Input username and password (QSW-2870 Switch initialized username is, "**admin"** and password is "**12345"**)
2. Designate IP address to QSW-2870 Switch for telnet user access.
3. Select [Start → Run] under Windows OS environment.
   Input command „telnet x.x.x.x" in the column of „Run" dialog, where „x.x.x.x" indicates IP address of the QSW-2870 Switch that has been designated in the above process.
4. Click <OK> to start telnet client. There will be pop-up login interface. If

the network connection is ok.

5. Input username and password (QSW-2870 Switch initialized username is „**admin'** and password is „**12345'**) to access into the command line interface for configuration, Successful:

1.3.3 Login through SSH

Purpose

This section introduces how to log into QSW-2870 Switch via SSH of local PC. The SSH login is available when user has higher security requirement.

Network Environment

The requirement of network environment to SSH login can be referenced to requirement of Console or telnet login.

Precondition

Before SSH login to QSW-2870 Switch, There is issue the user needs to confirm:

- The command „sshd" for enabling SSH facility has already been proceeded after a first power-up and device login via serial port.

1.3.3.1 Use Local Account and Password to Login by SSH

Process

1. Create SSH login (taking the example of Secure CRT implementation) by clicking button marked with red circle, referring to Figure Create SSH Login:

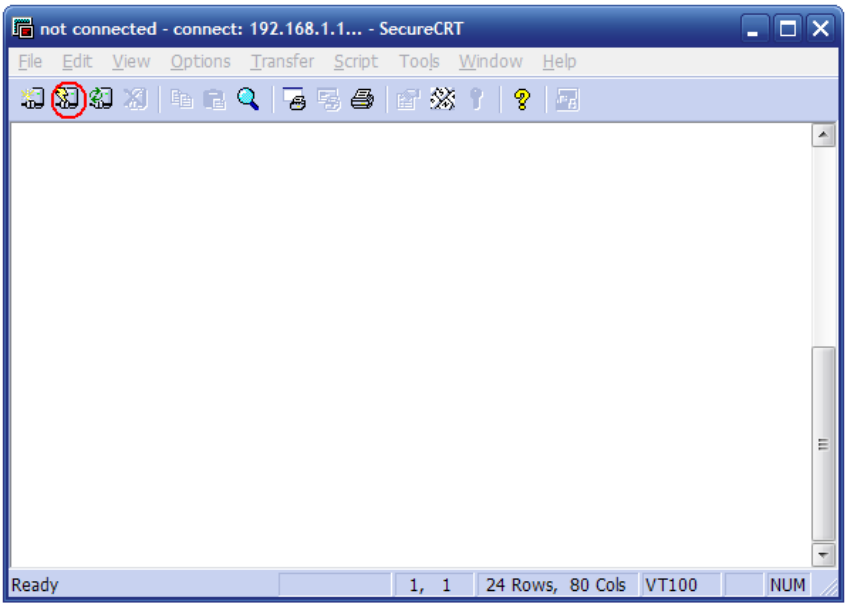


Figure Create SSH Login

2. Input relative parameters in the pop-up dialog of „Quick Connect", where the „Hostname" indicates inband IP address configured in the switch, while the „Username" indicates username of local user that was created in the device via command „username", referring to Figure Input SSH Parameters:

Figure Input SSH Parameters

3. Click the button of [Connect] and wait for a while until the user login interface appears, that the user is able to perform SSH login by inputting local user account including username and password. (It is suggested that to perform „ping" command for device connection availability before the login and connection)

Notice:

The above step from 1 to 3 is for user"s first time of SSH login. If the SSH has already been created, the following steps can be suggested for SSH login.

4. Click the button [Connect] from the Secure CRT interface directly, referring to red circle marked in Figure SSH Login (1):

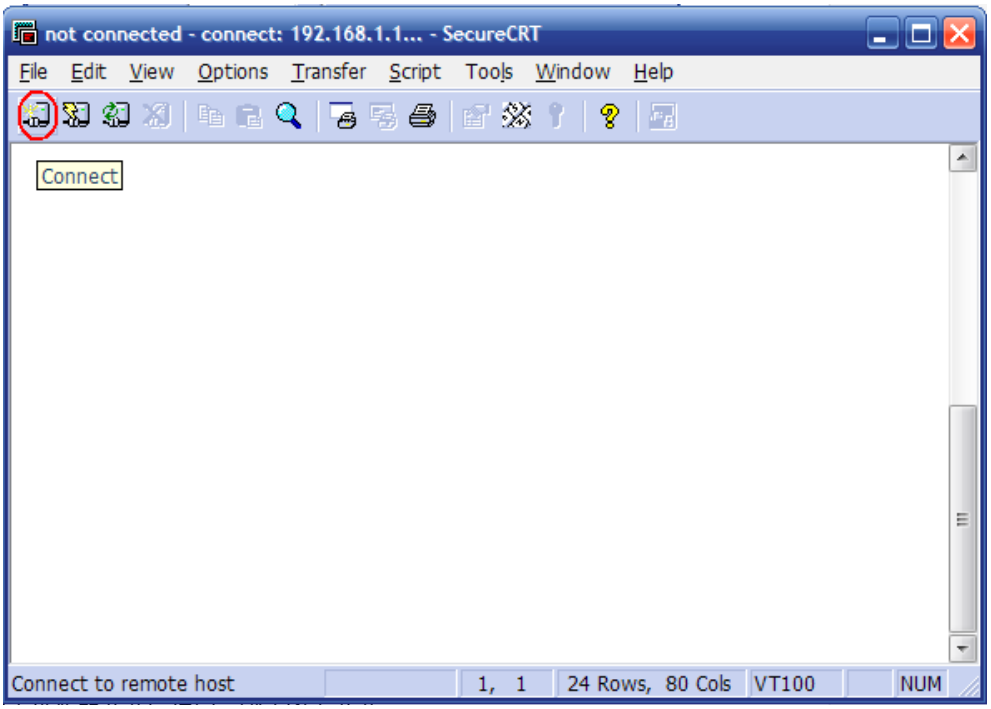


Figure SSH Login (1)

5. Select the area marked in red circle from pop-up [Connect] dialog, referring to Figure SSH Login (2), and click [Connect].

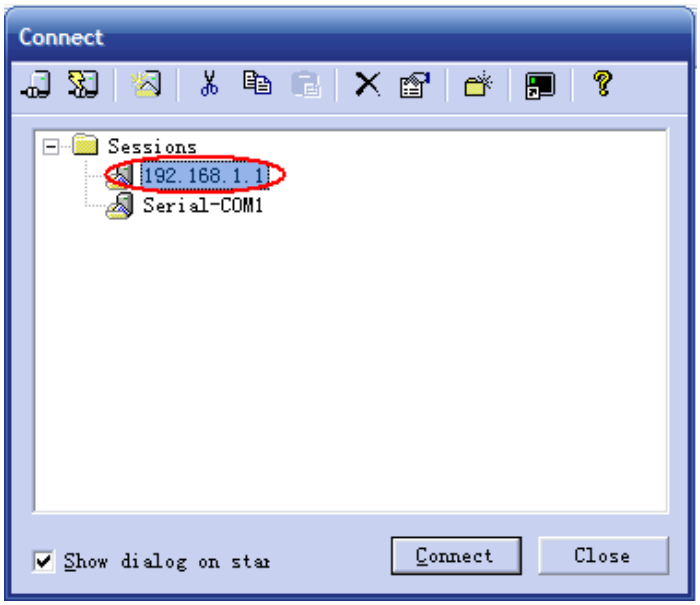


Figure SSH Login (2)

6. Input local password from pop-up dialog of [Connect to], referring to Figure Input of SSH Login Password. If „Save password" is selected, there will be no password input when logging next time.

Figure Input of SSH Login Password

Result

The SSH login will be successful if the settings are according to above steps, A Successful SSH Login with Local Username and Password:

1.3.3.2 Use Public Key to Login by SSH

Process

The following configuration steps are taking the example of Secure CRT implementation.

1. Create private/public key (generate public key via Secure CRT) by clicking option „Create Public Key" in the Tools of Secure CRT menu bar, referring to Figure Create Private/Public Key

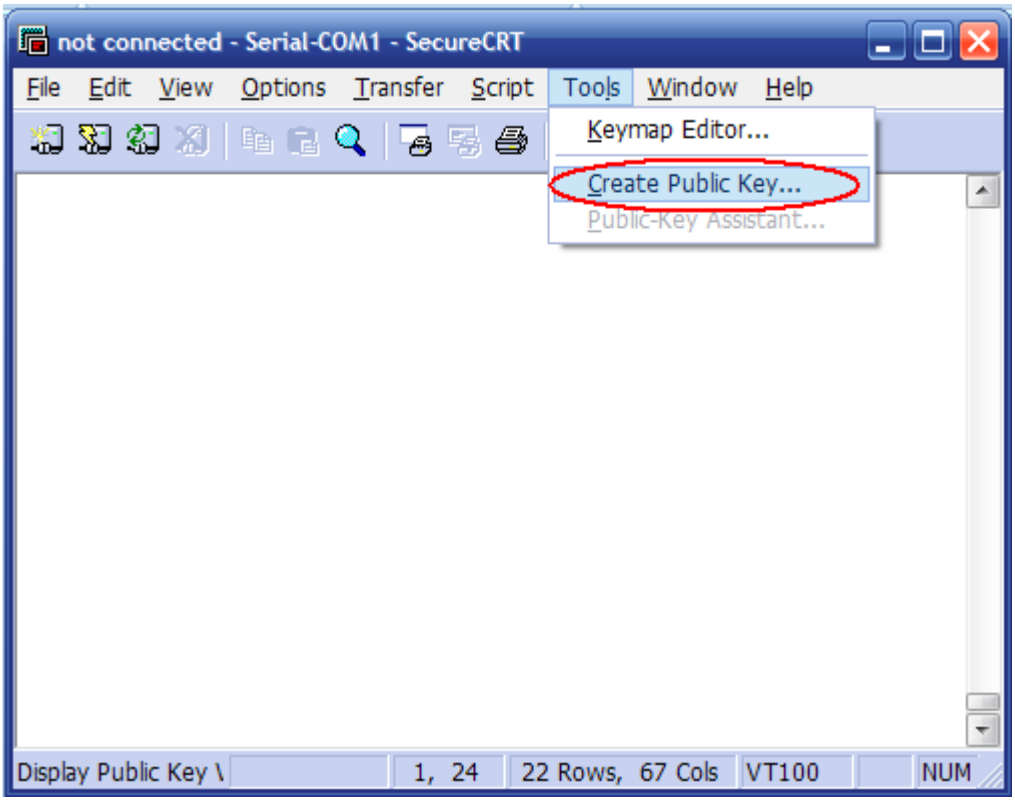


Figure Create Private/Public Key

2. Click „Next" button from pop-up dialog [Key Generation Wizard], referring to Figure Generate SSH Private/Public Key (1):

Figure Generate SSH Private/Public Key (1)

3. Select generation method by choosing „DSA" or „RSA" from the drop down menu of the dialog, and click „Next" for confirmation, referring to Figure Generate SSH Private/Public Key (2):

Figure Generate SSH Private/Public Key (2)

4. Input relative parameters, where the „Passphrase", „Confirm" and „Comment" can be input for new SSH key description, the value of „Passphrase" must be remembered however. Click „Next" for confirmation, referring to Figure Generate SSH Private/Public Key (3):

Figure Generate SSH Private/Public Key (3)

5. Select default parameter „1024" for the pop-up dialog and click „Next", referring to Figure 1-22 Generate SSH Private/Public Key (4):

Notice:

Key length that DSA supports is 512|768|1024|2048|3072 while the length supported by RSA is 768|1024|2048|3072.

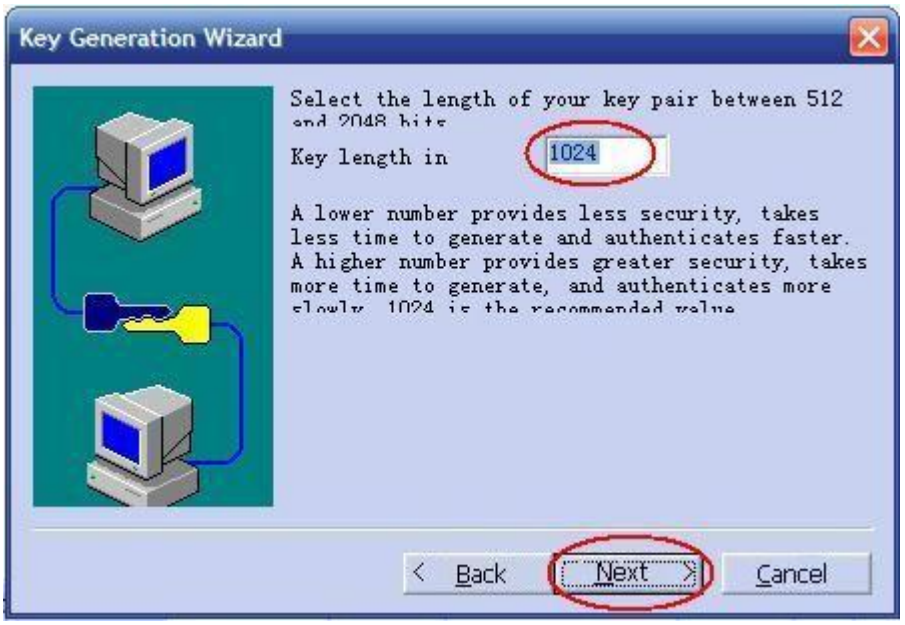


Figure Generate SSH Private/Public Key (4)

6. The generation of private/public key will be displayed in the pop-up dialog. Click „Next" button if the generation is finished, referring to Figure Generate SSH Private/Public Key (5):

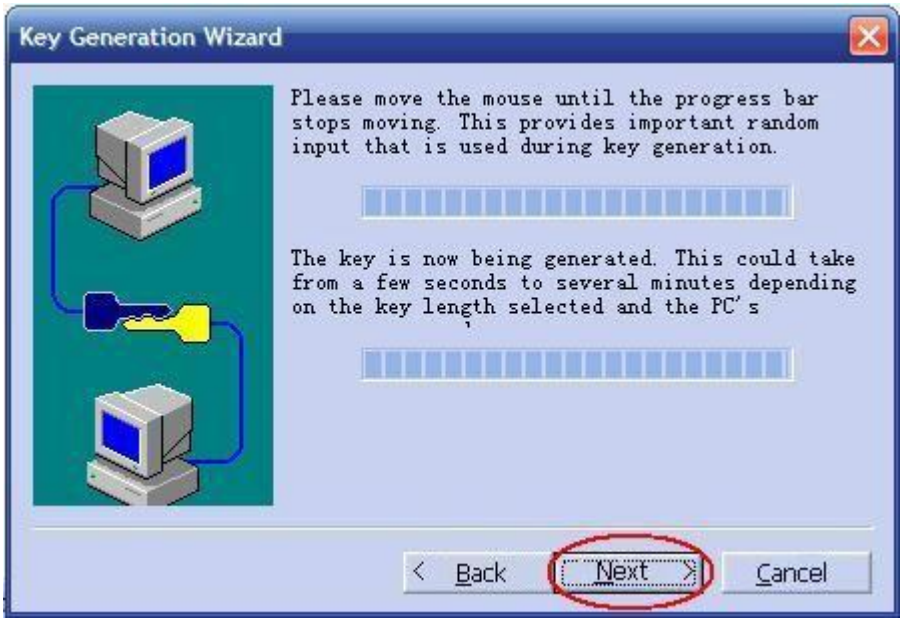


Figure Generate SSH Private/Public Key (5)

Notice:

It is suggested to keep moving mouse inside the area of private/public key generation dialog when the generation is running, otherwise the progress bar will be slow.

7. The saving path of initial public key document that is generated must be the default one that is recommended by the Secure CRT. Click „Done" to finish the generation, referring to Figure SSH Key Document Saving:

Figure SSH Key Document Saving

8. Modify the generated initial key document „Identity.pub" (Please refer to Appendix **A** for the modification of initial public key document) and download it into the device via FTP, referring to Figure FTP Download of Generated Initial Public Key:

```
192.168.1.11 (config)#ftp get 192.168.1.118 123 123 e:\Identity.pub
 Local path is "Ram:/flash/download".
 Getting data...
 588 bytes downloaded.

 If you want to update system,use "upgrade" command!
```

Figure FTP Download of Generated Initial Public Key

9. Copy the downloaded initial public key document to user category of the device, referring to Figure Copy the Initial Public Key to Designated User

Category, taking the admin user category as the example:

```
      #copy download user/admin/ssh_authorized_keys2
  %Copying file Ram:/flash/download -> Ram:/flash/user/admin/ssh_authorized_keys2
      #cd user
  %Current Directory is "Ram:/flash/user".
      #cd admin
  %Current Directory is "Ram:/flash/user/admin".
      #ls
Listing Directory Ram:/flash/user/admin:
   attr    link   uid     gid      size      date      time   name
---------- ---- ------- ------- --------- ---------- -------- -----
drwxrwxrwx 1    0       0            4096 1980-01-01 00:21:28 ./
drwxrwxrwx 1    0       0            4096 1980-01-01 00:21:28 ../
-rwxrwxrwx 1    0       0             588 1980-01-01 00:20:36 ssh_authorized_keys2

        1 files,2 directorys,total space:588 bytes

        available space: 2605056 bytes.
```

Figure Copy the Initial Public Key to Designated User Category

 Notice:

The file name of the public key document being stored in the device must be „sh_authorized_key2".

The admin user as default deployment usually exists in most of the telecommunication devices. Besides, user is also allowed to create other user accounts with types of authentication. If the created public key is copied into other user category, then the username and password (referring to step 11 in this section) must be input accordingly when logging via SSH.

10. Logging device via SSH by operating SSH client software (e.g., Secure CRT) at PC (or configuration terminal), referring to Figure SSH Login marked in red circle:

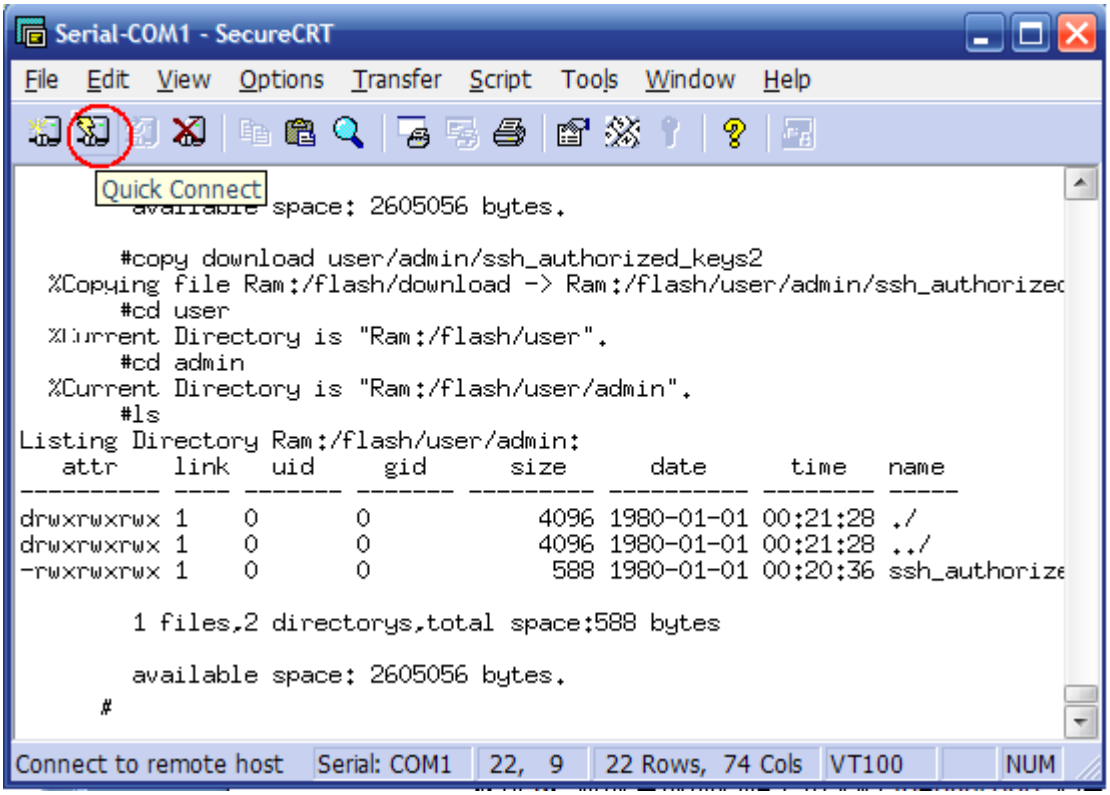


Figure SSH Login

11. In the following dialog, select „SSH2" for option „Protocol", device inband IP address for option „Hostname", user with public key document copied under corresponding category for option „Username", and „PublicKey" for column Primary of Authentication, and click button [Propertiers..], referring to Figure SSH Login Parameters Input (1):

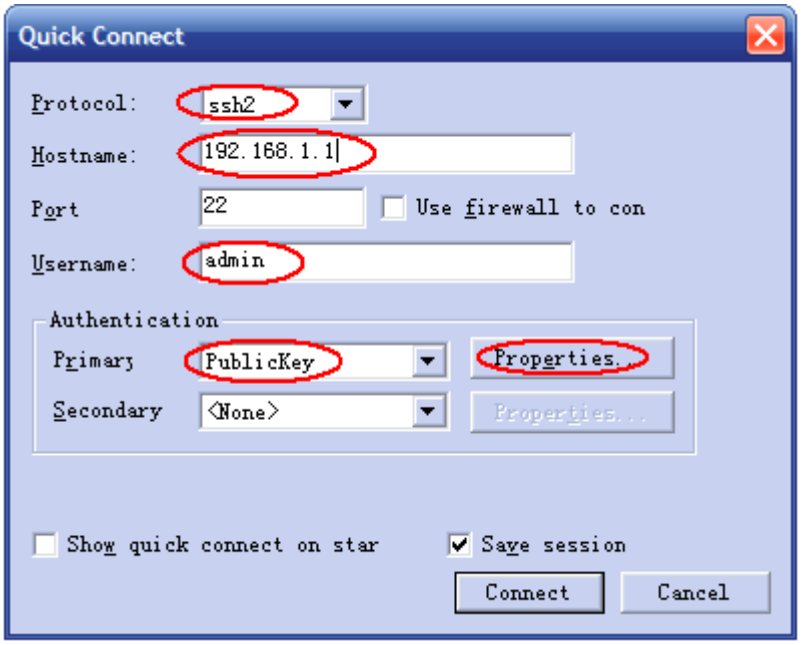


Figure SSH Login Parameters Input (1)

12. From the pop-up dialog, input the Passphrase that has been defined during the creation of public key dialog (i.e., value in Step 4), and click button [OK], referring to Figure SSH Login Parameters Input (2):

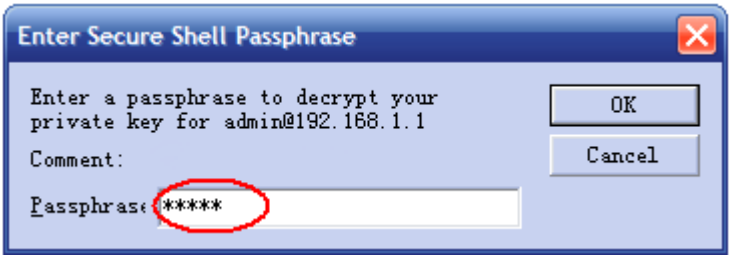


Figure SSH Login Parameters Input (2)

Notice:

The above way of SSH login via public key can be also implemented through command „**ssh keygen/sshd auth/ssh login method**" in the CLI, referring to <*Qtech QSW-2870 Series Carrier Class Layer-2 Ethernet Switch CLI User Manual*>.

Result

The SSH login will be successful by above configuration steps, referring to Figure 1-30 A Successful SSH Login via Public Key:

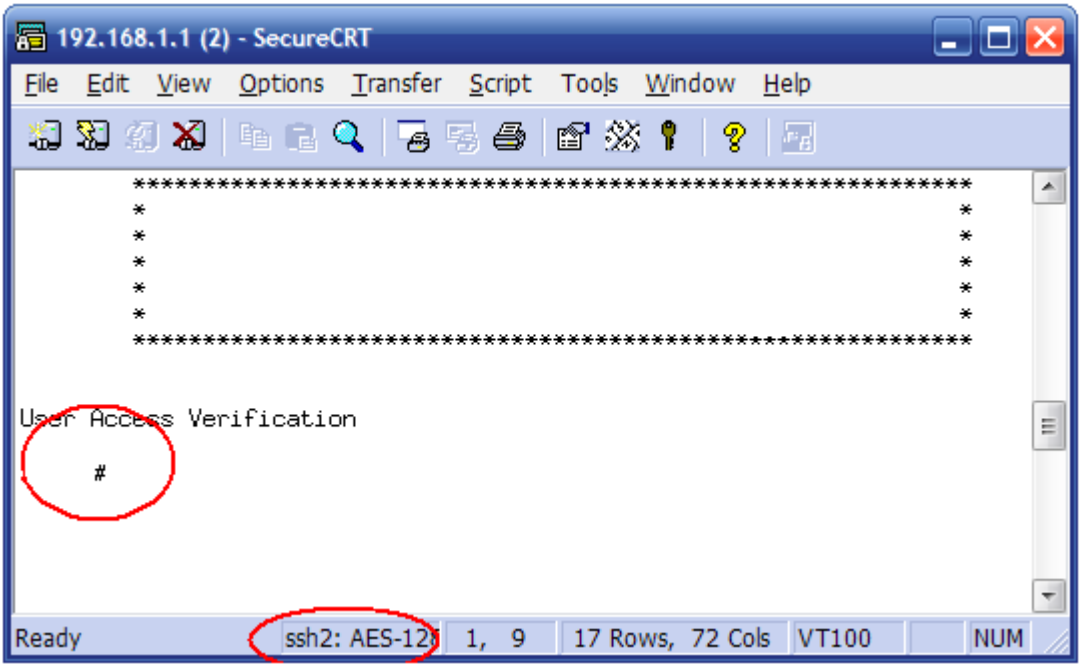


Figure A Successful SSH Login via Public Key

1.4 Device File Upload and Download

1.4.1 FTP Configuration

1.4.1.1 FTP Introduction

File Transfer Protocol (FTP) is a universal method of file transmission in the Internet and IP network. The file transmission provided by FTP is to copy a complete file from a system to another. The FTP supports limited file types (ASCII, binary, etc.) and file structures (byte flow oriented or record). Most users regularly prefer to Email and Web for file transmission at present however, FTP is still in wide spread use. The FTP protocol belongs to application layer protocol in TCP/IP protocol suite that it is applied for file transmission between remote server and local host. The FTP services that QSW-2870 Switch provides are including:

FTP Server: User is allowed to access FTP server and visit files within, by running FTP client to log into the server (before the user login, network administrator has to get IP address of FTP server configured in advance).

The FTP client provided by the switch as an application module belongs to an accessorial function for user that does not take responsibility of functional configuration. The switch as the FTP client at the time, connects with remote server, and corresponding operations (such as category create and delete and so on) can be achieved by typing FTP client commands.

FTP Client Service: After the connection with the switch (FTP Client) is established via PC terminal emulation program or telnet, the user is allowed to establish connection between switch and remote FTP server by inputting command „ftp x.x.x.x" (x.x.x.x indicates IP address of remote FTP server) so that to visit files in remote FTP server.

The QSW-2870 Switch supports FTP functionalities under two types of network address, IPv4 and IPv6.

1.4.1.2 Enable/Disable FTP Server

Purpose

This section introduces how to enable or disable FTP server.

Process

According to the different purposes, execute corresponding step. Please refer to the following table.

Purpose	Process
Enable server	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **ftpd** for device FTP server enabling; 3. Done.
Disable server	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **no ftpd** for device FTP server disabling; 3. Done.

1.4.1.3 FTP Upload File

Purpose

This section introduces how to upload file through FTP.

Process

According to the different purposes, execute corresponding step. Please refer to the following table.

Purpose	Step
(IPv4)Upload local file to remote FTP server	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **ftp put** *ipv4-address user password remotefile* **config** or use command of **ftp put** *ipv4-address user password remotefile* **localfile** *filename* [*port-id*] to upload local file to remote FTP server; 3. Done.
(IPv6)Upload local file to remote FTP server	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **ftp put** *ipv6-address user password remotefile* **config** or use command of **ftp put** *ipv6-address user password remotefile* **localfile** *filename* [*port-id*] to upload local file to remote FTP server; 3. Done.

Appended List:

Parameter	Description	Value
ipv4-address	Host IPv4 address	Dotted decimal
ipv6-address	Host IPv6 address	In the IPv6 address form, 128 bits IP address is distributed as 8 groups that 12 bits in each group is indicated with 4 hexadecimal characters (0~9, A~F) and separated with punctuation „:", where each „X" is indicating a group of hexadecimal value
user	Username for FTP service login	String form with length 1~63
password	Password for FTP service login	String form with length 1~63
remotefile	File name that is to be downloaded to the host	String form with length 1~63
filename	Designated local file name	String form with length 1~63
[port-id]	Port number, optional configuration	Integer form with value range between 1~65535
config	Device config file to be uploaded	-

1.4.1.4 FTP Download File

Purpose

This section introduces how to download file through FTP.

Process

According to the different purposes, execute corresponding step. Please refer to the following table.

Purpose	Step
(IPv4)Download remote file and save to local	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **ftp get** *ipv4-address user password remotefile* [*port-id*] or use command of **ftp get** *ipv4-address user password remotefile* **localfile** *filename* [*port-id*] or use command of **ftp get** *ipv4-address user password remotefile* **config** to download remote file and save to local; 3. Done.
(IPv6)Download remote file and save to local	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **ftp6 get** *ipv6-address user password remotefile* [*port-id*] or use command of **ftp6 get** *ipv6-address user password remotefile* **localfile** *filename* [*port-id*] or use command of **ftp6 get** *ipv6-address user password remotefile* **config** to download remote file and save to local; 3. Done.

Appended List:

Parameter	Description	Value
ipv4-address	Host IPv4 address	Dotted decimal
ipv6-address	Host IPv6 address	In the IPv6 address form, 128 bits IP address is distributed as 8 groups that 12 bits in each group is indicated with 4 hexadecimal characters (0~9, A~F) and separated with punctuation „:", where each „X" is indicating a group of hexadecimal value
user	Username for FTP service login	String form with length 1~63
password	Password for FTP service login	String form with length 1~63
remotefile	File name that is to be downloaded to the host	String form with length 1~63
filename	Designated local file name	String form with length 1~63
[port-id]	Port number, optional configuration	Integer form with value range between 1~65535
config	Device config file to be uploaded	-

1.4.1.5 FTP Delete File

Purpose

This section introduces how to delete file through FTP.

Process

According to the different purposes, execute corresponding step. Please refer to the following table.

Purpose	Step
(IPv4)Delete designate file of FTP server	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **ftp delete** *ipv4-addressuser password remotefile* or use command of **ftp delete** *ipv4-address user password remotefile* [*port-id*] to delete designated file of FTP server; 3. Done.
(IPv6)Delete designate file of FTP server	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **ftp6 delete** *ipv6-address user password remotefile* or use command of **ftp6 delete** *ipv6-address user password remotefile* [*port-id*] to delete designated file of FTP server; 3. Done.

Appended List:

Parameter	Description	Value
ipv4-address	Host IPv4 address	Dotted decimal
ipv6-address	Host IPv6 address	In the IPv6 address form, 128 bits IP address is distributed as 8 groups that 12 bits in each group is indicated with 4 hexadecimal characters (0~9, A~F) and separated with punctuation „:", where each „X" is indicating a group of hexadecimal value
user	Username for FTP service login	String form with length 1~63
password	Password for FTP service login	String form with length 1~63
remotefile	File name that is to be downloaded to the host	String form with length 1~63
[port-id]	Port number, optional configuration	Integer form with value range between 1~65535

1.4.1.6 FTP Server Example

Purpose

This section introduces the example that the switch as a FTP server, to implement config file backup and software upgrade.

Device	Configuration
Switch	Start FTP Server with configuration of username and password and so on
PC	Switch login through FTP client program

Network Requirement

Remote PC as the FTP client manipulates configurations to the switch as the FTP server:

Configuration of FTP with username „switch‟ and password „hello‟, and w/r authority to switch Flash root is assigned to the user. The inband or outband IP address of the switch is 1.1.1.1 and PC IP address is 1.1.1.2 that the switch and PC are routing available. The application program „switch.z‟ of the switch is stored in PC and it is uploaded from PC to the remote switch through FTP when the switch config file „config‟ is downloaded to the PC to implement configuration file backup.

Topology

Figure FTP Configuration Topology

Process

Switch configuration:

1. User logs into the switch (local login via Console port or remote login via telnet) and start the FTP service up:

```
QSW-2870#config
QSW-2870(config)#ftpd
```

Username and password configuration through command „adduser":

```
QSW-2870 (config)#adduser switch password hello
```

2. Start FTP client program at PC and establish FTP connection with the switch. Upload switch application „switch.z" to switch Flash root and download configuration file „config" from the switch. The FTP Client application shall be purchased and installed by the user.

```
C:\ftp 1.1.1.1
    220 FTP Server ready User
(1.1.1.1㉿none)): admin
331 Password required
Password:
230 User logged in
ftp>bin
200 Type set to I, binary mode
ftp> put switch.z
200 Port set okay
150 Opening BINARY mode data connection
226 Transfer complete
ftp: sends 3069212 bytes within 1.42Seconds 2158.38Kbytes/sec.
```

#fetch switch config file

```
ftp>ascii
200 Type is ASCII
ftp>get startcfg
150 Opening ASCII mode data connection
226 Transfer complete
ftp: receive 14251 bytes within 0.22Seconds 65.07Kbytes/sec.
```

 Notice:

If there is no sufficient switch Flash Memory, please delete the existing applications inside the Flash and upload again.

The PC as the FTP server transmits mirror file with bin format, and config file with ASCII format.

3. Upgrade operation to the switch after the upload is finished.

The user is able to use command „upgrade os" as auto-start application for next switch boot-up and reboot the switch, that the switch is able to implement auto-upgrade to its OS.

```
QSW-2870#config
QSW-2870 (config)#upgrade os
QSW-2870 (config)#quit
QSW-2870#reboot
```

1.4.1.7 FTP Client Example

Purpose

This section introduces the example of switch as FTP Client implementing config file backup and software upgrade.

Device	Configuration	Description	Parameter Description
Switch	Use command „ftp" directly to logging into remote FTP server	User fetches FTP username and password first, and logs into remote FTP server so that to fetch corresponding category and file. **ftp {put |get } ftp-sever src-file dest-file**	**put**: to upload client file to server. **get**: to download server file to client. *ftp-server is* indicating IP address of FTP server; ***dest-file*** indicates local filename while ***src-file*** indicates file name that is to be uploaded to server
PC	Start FTP server with configurations of username, password and user authority and so on		

Network Requirement

Remote PC as FTP server and the switch as FTP client with configuration:

FTP with username 123 and password 123; PC IP address is 10.18.1.2; The user is able to log into remote QSW-2870 switch via telnet and download switch application from the FTP server to switch Flash so that to implement remote upgrade to the switch.

Topology

Figure Network Topology of Switch as FTP Client

Process

#enter global configuration view and input command to conduct FTP connection by inputting correct username and password for FTP server login.

```
QSW-2870 (config)#ftp get 10.18.1.2 123 123 d:\upgrade.z
Local path is “Ram:/flash/download”.
  getting data…
3069212 bytes downloaded
```

#Download upgrading program to the „download‟ category of switch and process the upgrading through upgrading command. The new mirror file will take effect only after the switch is rebooted.

```
QSW-2870 (config)#upgrade os

WARNING:System will upgrade! Continue?[y/n]
  System now is upgrading, please wait.
  %Local path is “Ram:/flash/download”.
QSW-2870 (config)#reboot
```

1.4.2 TFTP Configuration

1.4.2.1 TFTP Introduction

Trivial File Transfer Protocol (TFTP) was initially introduced for no-disk system conducting (usually work station or X terminal). Comparing with another file transmission protocol FTP, the TFTP does not have complex interactive access interface or authority control that it is suitable for environment with no complex interaction between client and server. The TFTP protocol is usually implemented based on UDP.

The protocol transmission of TFTP is conducted by the client side. When file downloading is required, a request packet will be sent from client side to TFTP server and data will be received from the server along with confirmation towards it; when file uploading is required on the other side, request packet will be sent from the client side to the TFTP server and data will be received to the server along with confirmation from it. The transmission mode of TFTP is binary mode.

Before TFTP configuration, the network administrator needs to configure IP addresses of TFTP client side and server side, and make sure that the routing between client and server is available.

The QSW-2870 Switch supports TFTP functionality under two types of network address, IPv4 and IPv6.

Figure TFTP Configuration Topology (1)

1.4.2.2 Configure TFTP Server On-Off

Purpose

This section introduces how to open or close TFTP server of the switch.

Process

According to the different purposes, execute corresponding step. Please refer to the following table.

Purpose	Process
Start device TFTP server function	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **ttftpd** to start device TFTP server function; 3. Done.
Start device TFTP6 server function	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **ttftpd6** to start device TFTP6 server function; 3. Done.
Close device TFTP server function	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **no ttftpd** to close device TFTP server function; 3. Done.
Close device TFTP6 server	1. Use command of **configure** to enter the Global

Purpose	Process
function	Configuration View; 2. Use command of **no ttftpd6** to close device TFTP6 server function; 3. Done.

1.4.2.3 TFTP Upload File

 Notice:

It is suggested to operate the command under the guide of engineers and technicians.

Purpose

When the switch needs to upload file to TFTP server, the switch as client side sends request packet towards TFTP server and sends data to the server along with confirmation from it. The following commands can be applied for file upload.

Process

According to the different purposes, execute corresponding step. Please refer to the following table.

Purpose	Step
Upload local file to remote TFTP server (applied for IPv4).	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **tftp put** *ipv4-address remotefile* **config** or **tftp put** *ipv4-address remotefile* **localfile** *filename* [*port-id*] to upload local file to remote TFTP server; 3. Done.
Upload local file to remote TFTP server (applied for IPv6).	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **tftp6 put** *ipv6-address remotefile* **config** or **tftp6 put** *ipv6-address remotefile* **localfile** *filename* [*port-id*] to upload local file to remote TFTP server; 3. Done.

Parameter Description

Parameter	Description	Value
Ipv6-address	Host IPv6 address	Pure binary indication: 128 0s and1s with 16 bits for each group and 8 groups in total

Parameter	Description	Value
ipv4-address	Host IPv4 address	Dotted decimal
remotefile	File name to be uploaded from the host to server	String form with length 1~63
filename	Local file name to be uploaded	String form with length 1~63
[port-id]	Port number, optional configuration	Integer form with range between 1~65535
config	Device config file to be uploaded	-

1.4.2.4 TFTP Download File

 Notice:

It is suggested to operate the command under the guide of engineers and technicians.

Purpose

When file download is required, the client side sends request packet to the TFTP server and receives data from the server along with configuration towards it. In practical device operation and maintenance, it is usually required that the config file or OS is downloaded from the host to the device for config modification or OS upgrade. The command is applied for file downloading to the device..

Process

According to the different purposes, execute corresponding step. Please refer to the following table.

Purpose	Process
Download remote file via TFTP and save it to local (applied for IPv4)	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **tftp get** *ipv4-address remotefile* [*port-id*] or **tftp get** *ipv4-address remotefile* **localfile** *filename* [*port-id*] to download remote file via TFTP and save it to local; 3. Done.
Download remote file via TFTP and save it to local (applied for IPv6)	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **tftp6 get** *ipv6-address remotefile* [*port-id*] or **tftp6 get** *ipv6-address remotefile* **localfile** *filename* [*port-id*] to download remote file via TFTP and save it to local;

Purpose	Process
	3. Done.

Parameter Description

Parameter	Description	Value
ipv4-address	Host IPv4 address	Dotted decimal
Ipv6-address	Host IPv6 address	Pure binary indication: 128 0s and1s with 16 bits for each group and 8 groups in total
remotefile	File name to be downloaded from the host to server	String form with length 1~63
filename	Local file name to be uploaded	String form with length 1~63
[port-id]	Port number, optional configuration	Integer form with range between 1~65535

1.4.2.5 TFTP Client Example

Purpose

This section introduces the example of switch as TFTP client implementing config file backup and software upgrade.

Device	Configuration	Default Value	Configuration Description
Switch	Use command „tftp" directly to logging into remote TFTP server for file upload/download	-	TFTP is applied for environment with no complex interaction between client and server. Please make sure the routing between switch and TFTP server available.
PC	Start TFTP server with configurations to TFTP category	-	-

Network Requirement

The switch as TFTP client and PC as TFTP server; the TFTP server has been TFTP working category configured. Inband switch IP address is 1.1.1.1 and the port connecting with switch and PC is belonging to particular VLAN; PC IP address is 1.1.1.2. Application program „switch.z" is saved in the PC. The switch downloads „switch.z" from TFTP server through the TFTP and uploads switch config file to

„vrpcfg.txt" under TFTP server working category, so that to implement config file backup.

Topology

Figure TFTP Configuration Topology (2)

Process

1. TFTP server is started in PC and working category of TFTP server is configured.

2. Configurations at the switch:

#User logs into the switch (the switch login can be implemented through local console port as well as remote telnet).

```
QSW-2870#config
QSW-2870 (config)#tftp get 1.1.1.2 switch.z
QSW-2870 (config)#tftp put 1.1.1.2  vrpcfg.txt config
```

1.4.3 Zmodem Configuration

1.4.3.1 Zmodem Introduction

Zmodem is to process file upload/download through switch serial port. It is because of limited transmission rate to its serial port that the operation with large file transmission is not suggested.

1.4.3.2 Zmodem Upload File

Background Information

It is not suggested to process operation for file download/upload with large file transmission, due to its limited serial port transmission rate.

Precondition

- Device starts up in normal;
- Device login correct;
- If switch config file upload is required, it is necessary to save config file in advance to guarantee there is file „startcfg‟ under switch Flash.

Purpose

To implement file upload through device serial port with operation introduced in this section.

Process

According to the different purposes, execute corresponding step. Please refer to the following table.

Purpose	Step
Upload file to device via serial port	1. Use command of **configure to** enter the Global Configuration View; 2. Use command of **zmodem put localfile** *filename* or use command of **zmodem put config** to upload file to device via serial port; 3. Done.

Appended List:

Parameter	Description	Value
filename	Designated local file name to be uploaded	String for with length 1~63

1.4.3.3 Zmodem Download File

Background Information

It is not suggested to process operation for file download/upload with large file transmission, due to its limited serial port transmission rate.

Precondition

- Device starts up in normal;
- Device login correct;
- If switch config file download is required, it is necessary to save config file in advance to guarantee there is file „startcfg‟ under switch Flash.

Purpose

To implement file download through device serial port with operation introduced in this section.

Process

According to the different purposes, execute corresponding step. Please refer to the following table.

Purpose	Step
Download file from device via serial port	1. Use command of **configure to** enter the Global Configuration View; 2. Use command of **zmodem get** [**localfile** *filename*] to download file from the device via serial port; 3. Done.

Appended List:

Parameter	Description	Value
filename	Local file name to be downloaded	String for with length 1~63

Chapter2
Layer 2 Ethernet Configuration

2.1 Summary

This chapter introduces the layer two Ethernet basic function configuration of QSW-2870. This chapter includes the following section.

2.2 Ethernet Interface Configuration

2.2.1 Ethernet Interface Configuration Introduction

Ethernet interface configuration includes:

- Enter Ethernet Interface View
- Enable/Disable Ethernet interface
- Configure Ethernet interface duplex state
- Configure Ethernet interface rate
- Configure Ethernet interface flow control
- Configure Ethernet interface broadcast/multicast message suppression function
- Configure Ethernet interface rate suppression function
- Configure Ethernet interface priority
- Configure Ethernet interface the maximum transmission unit
- Descript Ethernet interface
- Enable Ethernet device inband network management address
- Display Ethernet interface state

2.2.2 Ethernet Interface Basic Attribute Configuration

2.2.2.1 Enter the Ethernet Interface View

Background

It needs to enter the Ethernet Interface Configuration View first and then configure the Ethernet Interface.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step	Parameter
Enter the Ethernet Interface Configuration View	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface interface-type interface-number** to enter one specified interface configuration view.	interface-type: fastethernet interface-number: <1-8>/<0-4>/<1-48>
Exit Ethernet interface view	Use command of **quit**	-

2.2.2.2 Open/Shutdown Ethernet Interface

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step
Close Ethernet port When the port is suspended, i.e., no cable connected for data transmission, please use command „shutdown" to close the port so that to avoid abnormal working status caused by disturbance.	1. Use command of configure to enter the Global Configuration View; 2. Use command of i**nterface interface-type interface-number** to enter one specified interface configuration view; 3. Use command of **shutdown** to close current Ethernet port.
Open Ethernet port When parameters of interface property are modified and new configuration has	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface interface-type**

Objective	Step
not been taken effect yet, the command „shutdown" and „no shutdown" can be used for interface close and restart to make the interface effective again.	**interface-number** to enter one specified interface configuration view; 3. Use command of **no shutdown** to open current Ethernet port.

2.2.2.3 Configure Ethernet Interface Duplex State

Background

If it is required that the port is able to receive data packet while sending, then the port can be provisioned as full-duplex mode; if port receiving and sending data packet is required to be separated, then it can be provisioned as half-duplex mode; similarly, if the port is configured as auto-negotiation, the duplex mode can be automatically negotiated by both the local port and peer port.

Precondition

Before using the command, the command „negotiation auto" must be used to implement that only when the fast Ethernet port is working under non-auto-negotiation mode that it can be configured as port duplex mode. Otherwise, there will be prompt from the device as „%Info: Please configure negotiation auto disable first".

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step	Parameter
Configure the Ethernet port working under full-duplex mode	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface interface-type interface-number** to enter one specified interface configuration view; 3. Use command of „**duplex full**" to designate the port is working under full-duplex mode	In default, when the Ethernet port is working under non-auto-negotiation mode, its working mode is full-duplex.
Configure the Ethernet port working under half-duplex mode	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface interface-type interface-number** to enter one specified interface configuration view; 3.Use command of „**duplex half'** to	

Objective	Step	Parameter
	designate the port is working under half-duplex mode	

2.2.2.4 Configure Ethernet Interface Rate

Background

The following command can be used to set the Ethernet port rate. When the port to be rate provisioned is working under auto-negotiation mode, its rate is auto-negotiated and determined by both the local port and peer port.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step	Parameter
Configure Ethernet port rate	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface interface-type interface-number** to enter one specified interface configuration view; 3. Use command of **speed 10/100/1000** to set different rates for the interface as respectively 10Mbit/s, 100Mbit/s and 1000Mbit/s.	In default, when the port is working under non-auto-negotiation mode, its rate is the maximum rate supported by the port type.

2.2.2.5 Configure Ethernet Interface Flow Control

Background

When local and peer switches both start function of flow control, the local switch sends message to peer switch to inform peer switch to stop sending message if congestion happens to local switch; on the other side the peer switch will stop message sending to local switch once it receives the inform message, and vice versa. The mechanism is able to avoid message loss. The following command can be used to enable or disable local Ethernet port flow control. Once disabled, the port will no longer send flow control frame to peer.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step	Parameter
Enable Ethernet port flow control	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface interface-type interface-number** to enter one specified interface configuration view; 3. Use command of **flow –control enable**	In default, the flow control status of Ethernet port is disabled.
Disable Ethernet port flow control	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface interface-type interface-number** to enter one specified interface configuration view; 3. Use command of **flow –control disable**	

2.2.2.6 Configure Ethernet Interface Broadcast/Multicast Message Suppression Function

Purpose

In order to prevent port congestion caused by flush of broadcast/multicast message, the switch provides storm suppression function to broadcast/multicast message. The user is allowed to restrain broadcast/multicast message by configuring bandwidth via the command.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step	Parameter
Configure broadcast/multicast/unknown unicast storm message suppression to Ethernet port.	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface interface-type interface-number** to enter one specified interface configuration view; 3. Use command of **storm-control { multicast | broadcast | dlf } 64kbps times** or **storm-control { multicast |**	In default, port has no rate limit to broadcast/multicast/unknown unicast message. broadcast: to process storm suppression to broadcast message; multicast: to process storm suppression to multicast message; dlf : multicast: to process storm suppression to unknown unicast message; 64kbps: indicates the

Objective	Step	Parameter
	broadcast | dlf } percent percent-value	bandwidth granularity of passing data packet is 64 Kpbs; times: indicates times of bandwidth granularity that the passing data packet occupies; percent: indicates percentages of bandwidth granularity that the passing data packet occupies; percent-value: indicates the percentage value of bandwidth granularity that the passing data packet occupies;
Cancel the provision of storm suppression	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface interface-type interface-number** to enter one specified interface configuration view; 3. Use command of **no storm-control { multicast | broadcast | dlf }**	

2.2.2.7 Configure Ethernet Interface Rate Suppression Function

Background

There are particular situations that port rate is required to be controlled so that to provide different bandwidth for different users. The function of rate suppression provides such ability. The particular input/output bandwidth control granularity may be different due to different interface type.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step	Parameter
Configure rate suppression function to Ethernet port	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface interface-type interface-number** to enter one specified interface configuration view; 3. Use command of **rate-limit *{in|out}* [*ratio*]**	In default, the port has no bandwidth suppression. in: bandwidth suppression to port ingress side; out: bandwidth suppression to port egress side; rate-limit: bandwidth control rate, times of 64 kbps.
Cancel the rate suppression configuration to Ethernet port	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface interface-type interface-number** to enter one specified interface configuration view; 3. Use command of **no rate-limit *{in|out}***	

Objective	Step	Parameter
		integer with range of 1~16000

2.2.2.8 Configure Ethernet Interface Priority

Background

By configuring the priority of different interfaces, it assures that the most important service cannot be influenced by delay or discard and guarantees the network efficient running at the same time.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step	Parameter
Configure Ethernet interface priority	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface interface-type interface-number** to enter one specified interface configuration view; 3. Use command of **priority [*level*]**	interface default priority to be 0

2.2.2.9 Configure Ethernet Interface MTU

Background

When exchanging data in high throughput such as file transmission, it may encounter the long frame more than the standard Ethernet frame length. Use the following command to configure the frame size.

The MTU of Ethernet interface only influences the IP packaging on Ethernet interface or packet disassembly. The MTU of using Ethernet _II form is 1500. The MTU of using Ethernet _SNAP form is 1492.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step	Parameter
Configure the MTU of Ethernet	1. Use command of **configure** to enter the Global Configuration View;	MTU, integer with range of 64-9000, unit:

Objective	Step	Parameter
interface	2. Use command of **interface interface-type interface-number** to enter one specified interface configuration view; 3. Use command of **mtu *mtu***	byte MTU default to be 1522
Recover to be the default MTU	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface interface-type interface-number** to enter one specified interface configuration view; 3. Use command of **no mtu**	

2.2.2.10 Configure Cable Type Adaptation

Purpose

When the connection cable type of interface needs to match with the real used cable type, it needs to configure the connected cable adaption method. Interface does not support cross cable type default.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step
Configure interface only to adapt crossing cable type	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface interface-type interface-number** to enter one specified interface configuration view; 3. Use command of cross enable.
Configure interface only to adapt direct cable type	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface interface-type interface-number** to enter one specified interface configuration view; 3. Use command of **cross disable**.

2.2.2.11 Clear Current Ethernet Interface Statistics Information

Purpose

Use this section operation to clear the statistics information of current Ethernet interface when there is a large amount of information to be cleared.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step
Clear the statistics information of current Ethernet interface	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface interface-type interface-number** to enter one specified interface configuration view; 3. Use command of **reset counter.**

2.2.2.12 Descript Ethernet Interface

Purpose

Use the following command to configure interface description character string to distinguish each port.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step	Parameter
Configure Ethernet interface description character string	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface interface-type interface-number** to enter one specified interface configuration view; 3. Use command of **description description**	no description information default description: interface description information, character string, not support blank, case sensitive
Delete Ethernet interface description character string	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface interface-type interface-number** to enter one specified interface configuration view; 3. Use command of **no description description**	

2.2.3 Ethernet Interface Senior Attribution Configuration

2.2.3.1 Configure Interface Loopback Detection

Purpose

Use the following configuration task to enable interface loopback monitoring function and configure the interval of timing monitoring outside loopback situation so as to timing monitor each interface whether to be outer loop. If finding one interface to be loop, Switch will make this interface be in controllable working state.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step	Parameter
Globally disable or automatically recover loopback detection	loop-check action (port-block|vlan-block) This command is used to configure the dealing way of loop interface after finding the loop.	port-block: block interface of loopback vlan-block: block VLAN which the loop interface is in.
Globally enable/disable the trap alarm of interfaceloopback detection	loop-check trap (enable|disable)	-
Specify to detect loopback on which VLAN	loop-check vlan *<1-4094>*	
Enable/disable interface loopback detection	loop-check (enable|disable)	
re-enable interface loopback detection	loop-check *reset*	
debug interface loopback detection	show loop-check	display the global information of interface loopback detection
	show loop-check interface	display loopback detection information of all interfaces

2.2.3.2 Display Ethernet Interface State

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step
Check Ethernet Interface state	1. Enter the Common User View, the Privilege User View, the Global Configuration View or Interface Configuration View; 2. Use command of **show interface fastethernet *interface-number* config**
Check the basic information of all Ethernet Interface sand trunk interface	1. Enter the Common User View, the Privilege User View, the Global Configuration View or Interface Configuration View; 2. Use command of **show interface verbose**

2.2.3.3 Switch to Different Ethernet Interface Configuration View

Purpose

After configuring the attributes of the current interface, this section operation can be used to configure attributes of other interfaces.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step
Switch to new Ethernet Interface Configuration View from current Ethernet Interface Configuration View	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface interface-type interface-number** to enter the Interface Configuration View; 3. Use command of **switch fastethernet interface-number**

2.3 MAC Table Configuration

In order to quickly forward message, Switch needs to maintain MAC address table. The MAC address table includes the MAC address of device connected with Switch and the interface number of Switch connected with the device. The dynamic item (not configured manually) in the MAC address table is learned by Switch. The method of Switch learning MAC address is as the following. If one port (supposed to be portA) receives a data frame, Switch will analyze the source MAC address of this data frame (supposed to be MAC-SOURCE) and consider that the message with the destination MAC address of MAC-SOURCE can be forwarded by portA. If MAC-SOURCE has been existed in the MAC address table, Switch will update the corresponding table. If MAC-SOURCE has not been

included in the MAC address table, Switch will add this new MAC address (and the corresponding forwarding port of this MAC address) into the MAC address table.

For the message which destination MAC address can be found in the MAC address table, system will use hardware to forward directly. For the message which destination MAC address cannot be found in the MAC address table, system will forward the message in broadcast mode. After broadcasting, the message reaches the network device corresponding to this destination MAC address. The destination network device will respond to this broadcast message and the responding message includes the MAC address of this device. Switch adds the new MAC address into the MAC address forwarding table by address learning. The subsequent messages to the same destination MAC address will be directly forwarded by using this newly added MAC address item.

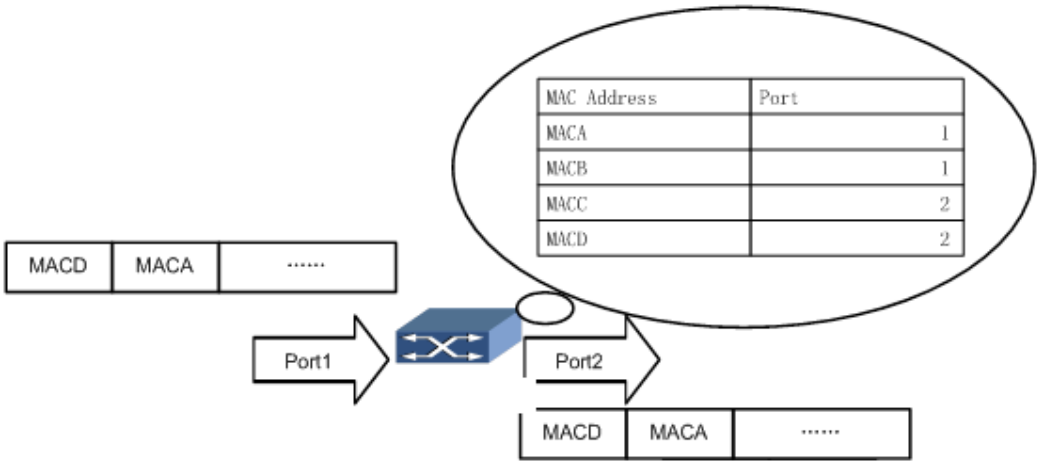


Figure Switch Uses Forwarding Table to Transmit Message

2.3.1 Configure MAC Address Table

Purpose

Administrator can add, modify or delete MAC address item in the MAC address table according to the real situation.

Use static MAC address to bind user device with interface. This can prevent the illegal user with fake identity from obtaining data and increase device security.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step	Parameter
Add/modify address item	1. Use command of **configure** to enter the Global Configuration View; 2. Use the following command: **mac-static vlan-id mac-address fastethernet interface-number**	vlan-id VLAN: integer with range of 1~4094 mac-address: static MAC address, form as AA:BB:CC:DD:EE:FF, A~F is one hex number interface-number: Ethernet interface number, integer with range of <1-8>/<0-4>/<1-48>

2.3.2 Configure System MAC Address Aging Time

Background

The appropriate aging time can realize the MAC address aging function effectively. The longer or shorter aging time configured by user may result in that Switch will broadcast many data messages which cannot find destination MAC address and it will influence the running performance of Switch. If user configures the aging time too long, Switch may save many old MAC address items and this will exhaust MAC address table resources and cause that the Switch cannot update MAC address table according to the changes in the network. If user configures the aging time too short, Switch may delete effective MAC address item.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Notice:

Once the system is reset, dynamic list will be lost, but the stored static list and black hole list will not be aged and lost.

Objective	Step	Parameter
Configure the aging time of MAC address table item	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **mac aging-time aging-time.**	default of system dynamic MAC address table item to be 300s aging-time: integer with range of 60~630, unit: second

2.3.3 Display Layer 2 MAC Address Table

Purpose

This section introduces how to quickly locate the relevant information of the specified MAC table item for user to query for specific information conveniently.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step	Parameter
Check Layer-2 static forwarding table	1. Enter the Common User View, the Privilege User View or the Global Configuration View; 2. Use one of the following commands: show mac-address MAC show mac-address MAC vlan VID show mac-address config show mac-address verbose	VID: VLAN id, optional, integer with range of 1~4094 MAC: static MAC address, form as AA:BB:CC:DD:EE:FF, A~F is one hex number config: means to display MAC address configuration information; verbose: means to display detailed MAC information except MAC configuration information

2.4 ARP Configuration

ARP mapping table can dynamically be maintained or manually maintained. Usually map the IP address manually configured to MAC address, it is called static ARP. User can check, add and delete ARP mapping item in ARP table by related manually maintained commands.

2.4.1 Add/Delete Static ARP Mapping Item Manually

Purpose

This section introduces how to add/delete static ARP mapping table manually.

Static ARP mapping table can only be configured manually and will not be influenced by ARP mapping table aging time and at the same time also cannot dynamically update this mapping relationship. Static ARP mapping table continues to be effective during the working time of device.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Procedure	Parameter
Add static ARP mapping table	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface vlan N1** to enter the vlan N1 Configuration View; 3. Use command of **ip arp ip-address mac-address fastethernet interface-number**;	system ARP table default to be empty, obtain address mapping by dynamic ARP ip-address: static ARP mapping IP address, dotted decimal mac-address: static ARP mapping MAC address, to be one hex interface-number: Ethernet interface number, integer, <1-8>/<0-4>/<1-48>
Delete static ARP mapping item	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface vlan N1** to enter the vlan N1 Configuration View; 3. Use command of **no ip arp ip-address**;	

2.4.2 Clear Dynamic ARP Table

Purpose

This section introduces how to clear dynamic ARP mapping table.

This section helps user to delete device all dynamic ARP mapping table items manually when necessary.

Execute this command to cancel the mapping relationship of IP address and MAC address and may result in that user cannot access some nodes, so user needs to use this command carefully.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step
Clear dynamic ARP mapping table	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **flush arp dynamic.**

2.4.3 Check ARP Information

Purpose

This section introduces how to check ARP related information. This section helps user to check ARP mapping table in LAN and detect fault of LAN. ARP established corresponding relationship between network address and local hardware address. Each corresponding record keeps a period of time in cache and then gives up.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step
Check ARP information	1. Enter the Common User View, the Privilege User View or the Global Configuration View; 2. Use command of **show ip arp**.

2.4.4 Configure Dynamic ARP Mapping Item Aging Time

Purpose

This section introduces how to configure the aging time of dynamic ARP mapping item.

The aging time of ARP mapping item can reduce the address parse error problem that the dynamic ARP table is not updated in time.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step	Parameter
Add static ARP mapping table	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **ip arp aging-time { aging-time | default }.**	default to be 1200s aging-time: aging time of dynamic ARP mapping item, integer with range of 60~1200, unit: second

2.4.5 Debug ARP

Purpose

This section introduces how to debug ARP.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step	Parameter
Enable ARP debug	Use command of **debug arp { in | out | error | all }** or **debug arp { dst-addr | src-addr } ip-address**	{ in | out | error | all |dst-addr | src-addr }: received packet, sent packet, error packet and all packets. ip-address: destination or source IP address, dotted decimal, form as IPv4: A.B.C.D
Disable ARP debug	Use command of **no debug arp { in | out | error | all }** or **no debug arp { dst-addr | src-addr } ip-address**	

2.5 Link Aggregation Configuration

2.5.1 Interface Aggregation Introduction

Link aggregation is to aggregate multiple ports into one single aggregation trunk group to implement egress load sharing of each member ports as well as provide high connecting reliability. Link aggregation can be divided into manual aggregation, dynamic aggregation and static LACP aggregation. Pots in a same aggregation trunk group shall have a same port type, i.e., if one of the ports is electric/optical port, all the others must be the same.

The QSW-2870 is currently supporting manual aggregation and static LACP aggregation only.

2.5.2 Configure Aggregation Group

Background

Please make sure that there is no member port inside the Trunk group before altering Trunk group work mode, otherwise, the change of work mode is unavailable. To delete existing member port, please use the command **no join trunk trunk-id** under corresponding configuration view, or run command **remove interface-type interface-number** under Trunk configuration view.

Purpose

Operations in this section can be used to provision Trunk group with its basic functions, as well as add member ports for enhancement of bandwidth and reliability.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step
Create Trunk and enter its configuration view	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface trunk** *trunk-id* to create aggregation group and enter its configuration view, if the group to be created has existed already, then enter its configuration view directly; 3. Done.
Configure Trunk working mode to be static LACP mode	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface trunk** *trunk-id* to enter the Trunk Interface Configuration View 3. Use command of **mode lacp-static to** configure Trunk working mode to be static LACP mode; 4. Done.
Add member interface into Trunk	Method1: 1.Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface trunk** *trunk-id* to enter the Trunk Interface Configuration View; 3. Use command of **add interface-type** { *interface-number1 [to interface-number2*] } to add member interface; 4. Done. Method2: 1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface interface-type** *interface-number* to enter the Interface Configuration View; 3. Use command of **join trunk** *trunk-id* to add the current interface into Trunk; 4. Done.
(Optional) Configure the load sharing mode	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface trunk** *trunk-id*, to access trunk interface view; 3. Use command of **load-balance** { dst-ip | dst-mac | src-ip | src-mac | src-dst-ip | src-dst-mac } to configure the load sharing mode of trunk; 4. Done.
(Optional)	Configure the high threshold value of active interface.

Objective	Step
Configure the threshold value of active interface	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface trunk** *trunk-id* to enter the Trunk Interface Configuration View; 3. Use command of **active-linknumber max** *link-number* to configure the high threshold value of active interface; 4. Done. Configure the low threshold value of active interface. 1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface trunk** *trunk-id* to enter the Trunk Interface Configuration View; 3. Use command of **active-linknumber min** *link-number* to configure the low threshold value of active interface; 4. Done.
(Optional) Configure system LACP priority	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **lacp priority** *system-priority* to configure system LACP priority; 3. Done.
(Optional) Configure interface LACP priority	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface interface-type** *interface-number* to enter the Interface Configuration View; 3. Use command of **lacp priority** *port-priority* to configure interface LACP priority; 4. Done.

Appendix List:

Parameter	Description	Value
trunk-id	trunk ID	integer with range of 1~8
interface-number	specify the observed Ethernet interface number	integer, <1-8>/<0-4>/<1-48>
link-number	specify link aggregation active interface high and low threshold value	integer with range of 1~8, active interface number default high threshold value to be 8, active interface number default low threshold value to be 1
system-priority	specify system LACP priority	integer with range of 0~65535, default system LACP priority to be 32768
port-priority	specify interface LACP priority	integer with range of 0~65535,

Parameter	Description	Value
trunk-id	trunk ID	integer with range of 1~8
		default interface LACP priority to be 32768

2.5.3 Maintenance and Debug

Purpose

When LACP function is abnormal, it needs to check and debug.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step
Enable LACP debug function	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter the Interface Configuration View or keep the current Privilege User View; 2. Use command of **debug lacp** { timer|event|churn|mux|rx|tx|logic|sync|all } to enable LACP debug function; 3. Done.
Disable LACP debug function	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter the Interface Configuration View or keep the current Privilege User View; 2. Use command of **no debug lacp** { timer|event|churn|mux|rx|tx|logic|sync|all } to disable LACP debug function; 3. Done.
Check LACP configuration file information	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter the Interface Configuration View or keep the current Privilege User View; 2. Use command of **show lacp config** to display LACP configuration file information; 3. Done.
Check all or	1. Use command of **disable** to exit to the Common User View or use

Objective	Step
specified LACP group information	command of **configure** to enter the Global Configuration View or use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter the Interface Configuration View or keep the current Privilege User View; 2. Use command of **show lacp trunk** [*trunk-id*] to display all or specified LACP group information; 3. Done.
Check related configuration information of LACP	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter the Interface Configuration View or keep the current Privilege User View; 2. Use command of show lacp system to display related configuration information of LACP ; 3. Done.

Appendix List:

Parameter	Description	Value
rx	received data packet	-
tx	data packet sent	-
timer	timer	-
event	event notification	-
churn	churn state machine	-
mux	Muxstate machine	-
logic	choice logic	-
sync	synchronization	-
all	all information	-

2.5.4 Example

Network Requirement

Configure link aggregation group on two directly connected Switches to increase the bandwidth and reliability between the two devices. And the detailed requirements are as the following.

- The link between two devices has the ability of redundant backup. When part of the links is failed, the backup link can be used to replace the fault link and keep the transmission no-break.

- Active link has the ability of load sharing.

Network Topology

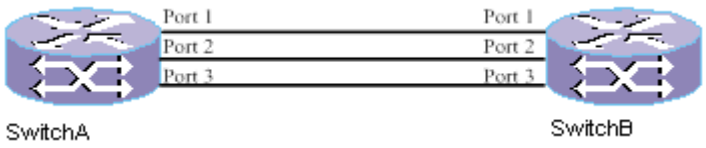


Figure LACP Configuration Topology

Configuration Step

Note: The configuration of two peers is the same and this only display configuration of one peer.

```
1. Create LACP aggregation group.
SX(config)#interface trunk 1/1
SX(config-trunk1/1)#no shutdown
SX(config-trunk1/1)#join vlan 1 untagged
SX(config-trunk1/1)#mode –static
2. Add interface 1-3 to the trunk group.
SX(config)#interface fastethernet 1/0/1 to fastethernet 1/0/3
SX(config-ge1/0/1->ge1/0/3)#no shutdown
SX(config-ge1/0/1->ge1/0/3)#join vlan 1 untagged
SX(config-ge1/0/1->ge1/0/3)#join trunk 1/1
3. Configuration finishes and check the trunk group information.
SX#show lacp trunk 1/1
eth-trunk 1:
        LACP Status: master        Port number: 3

fastethernet-1/0/1
  Port Status: Up and bind
  Flag: S – Device is sending Slow LACPDUs
        F – Device is sending fast LACPDUs
  Local information:
        Mode        Flags    Priority   AdminKey   OperKey    PortId   State
        active      F        32768      0x19       0x19       0x1      0xa9d7f8
  Partner"s information:
        Port   Flags    SysPri     PortPri    AdminKey   OperKey    OperPort OperState DevID
        1      F        32768      32768      0x0        0x19       0x1      0x9dfb6c  0x00046798185d
```

```
fastethernet-1/0/2
  Port Status: Up and bind
  Flag: S – Device is sending Slow LACPDUs
        F – Device is sending fast LACPDUs
  Local information:
        Mode        Flags    Priority   AdminKey   OperKey    PortId   State
        active      F        32768      0x19       0x19       0x2      0xa9d7f8
  Partner"s information:
        Port    Flags    SysPri     PortPri    AdminKey   OperKey   OperPort  OperState  DevID
        2       F        32768      32768      0x0        0x19      0x2       0x9dfb6c   0x00046798185d

fastethernet-1/0/3
  Port Status: Up and bind
  Flag: S – Device is sending Slow LACPDUs
        F – Device is sending fast LACPDUs
  Local information:
        Mode        Flags    Priority   AdminKey   OperKey    PortId   State
        active      F        32768      0x19       0x19       0x3      0xa9d7f8
  Partner"s information:
        Port    Flags    SysPri     PortPri    AdminKey   OperKey   OperPort  OperState  DevID
        3       F        32768      32768      0x0        0x19      0x3       0x9dfb6c   0x00046798185d
```

2.6 VLAN Configuration

2.6.1 VLAN Introduction

VLAN Meaning

Divide LAN (Local Area Network) into multiple subclasses in logic and each subclass has its own broadcast domain that is VLAN (Virtual Local Area Network).

Generally speaking, VLAN divides the devices in the LAN into multiple network segments logically but not physically to realize the isolated broadcast domains in a LAN technologically.

VLAN Function

- Isolate broadcast domain and reduce broadcast storm and enhance the security.
- In the large scale of network, it can restrict the network fault in VLAN and enhance the network robust.

2.6.2 Create VLAN

Purpose

This section introduces how to create VLAN and it is the basic precondition for other VLAN function configuration.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step
Create and enter the VLANIF Configuration View	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface vlan** *vlan-id* to create and enter the VLANIF Configuration View; 3. Done.
Delete the specified VLANIF	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **no interface vlan** *vlan-id* to delete the specified VLANIF View; 3. Done.
Create VLAN and enter the VLAN Configuration View	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **vlan** *vlan-id1* [*vlan-id2*] to create one or more VLAN and enter the VLAN Configuration View; 3. Done.
Delete one VLAN or VLAN in batches	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **no vlan** *vlan-id1* [*vlan-id2*] to delete one VLAN or VLAN in batches; 3. Done.
Switch VLAN configuration view	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **vlan** *vlan-id1* [*vlan-id2*] to create one or moer VLAN and enter the VLAN Configuration View; 3. Use command of **switch vlan** *vlan-id* to create other VLAN in VLAN Configuration Viewand enter the created VLAN Configuration View; 4. Done.

Appendix List:

Parameter	Description	Value
vlan-id	VLAN ID	integer with range of 1~4094

2.6.3 Configure VLAN Based on Interface

Purpose

This section introduces how to configure VLAN based on interface.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step
Configure the default VLAN of interface and configure the interface to join in the default VLAN	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter the Interface Configuration View; 3. Use command of **port default vlan** *vlan-id* to configure the default VLAN of interface and configure the interface to join in the default VLAN; 4. Done.
Configure the VLAN wich Hybrid interface belongs to	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter the Interface Configuration View; 3. Use command of **port hybrid vlan** *vlan-list* { **tagged** | **untagged** } to configure the VLAN which Hybrid interface belongs to; 4. Done.
Configure the default VLAN of Hybrid interface	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter the Interface Configuration View; 3. Use command of **port hybrid pvid** { *vlan-id* | **default** } to configure the default VLAN of Hybrid interface; 4. Done.
Configure the link type of interface	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter the Interface Configuration View; 3. Use command of port link-type { access | trunk | hybrid | default } to configure the link type of interface; 4. Done.
Configure trunk interface to join in VLAN	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter the Interface Configuration View; 3. Use command of **port trunk allow-pass vlan** *vlan-list* to configure trunk interface to join in VLAN; 4. Done.
Configure the default VLAN of trunk interface	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter the Interface Configuration View; 3. Use command of **port trunk pvid** { *vlan-id* | **default** } to configure the

Objective	Step
	default VLAN of trunk interface; 4. Done.

Appendix List:

Parameter	Description	Value
vlan-id	VLAN ID	integer with range of 1~4094
vlan-list	specify the VLAN list of trunk interface	form as 1,3,5~8, integer with range of 1~4094
default	the VLAN ID of trunk interface recover to be the default value	default:1, default to be VLAN1

2.6.4 Configure VLAN Based on MAC Address

Purpose

This section introduces how to configure divided VLAN based on MAC address.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step
Enable or disable divided VLAN based on MAC address of interface	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter the Interface Configuration View; 3. Use command of **mac-vlan** { **enable** | **disable** } to enable or disable divided VLAN based on MAC address of interface; 4. Done.
Configure interface to allow VLAN based on MAC address to pass	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter the Interface Configuration View; 3. Use command of **port link-type hybrid** to configure interface link type to be hybrid; 4. Use command of **port hybrid vlan** *vlan-list* **untagged** } to configure Hybrid interface to join in the VLAN based on MAC address; Done.
Configure to associated MAC address	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **mac-vlan** *mac-address/mac-mask vlan-id* **priority**

Objective	Step
with VLAN and at the same time configure the corresponding VLAN 802.1p priority with MAC address	*priority* or use command of **mac-vlan** *mac-address/mac-mask vlan-id* to configure to associated MAC address with VLAN and at the same time configure the corresponding VLAN 802.1p priority with MAC address ; 3. Done.

Appendix List:

Parameter	Description	Value
mac-address	specify the associated MAC address with VLAN	Form as AA:BB:CC:DD:EE:FF, A~F is a hex
mac-mask	specify MAC address mask	Form as FF:FF:FF:FF:FF:FF
vlan-id	specify the associated VLAN ID with MAC address VLAN ID	integer with range of 1~4094
priority	specify corresponding VLAN 802.1p priority with MAC address	integer with range of 0~7, the value is bigger and the priority is higher, default to be 0

2.6.5 Configure VLAN Based on IP Sub-network

Purpose

This section introduces how to configure VLAN divided based on IP sub-network.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step
Enable or disable divided VLAN based on IP sub-network	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter the Interface Configuration View; 3. Use command of **ip-subnet-vlan** { **enable** | **disable** } to enable or disable divided VLAN based on IP sub-network; 4. Done.
Configure interface to allow VLAN base on IP sub-network to pass	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter the Interface Configuration View; 3. Use command of **port link-type hybrid** to configure the link type to be hybrid; 4. Use command of **port hybrid vlan** *vlan-list* **untagged** } to configure

Objective	Step
	Hybrid type interface to join in the VLAN based on IP sub-network; Done.
Configure VLAN based on IP sub-network and at the same time configure corresponding VLAN 802.1p priority of IP sub-network	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **ip-subnet-vlan** *ip-address mask-address vlan-id* **priority** *priority* or use command of **ip-subnet-vlan** *ip-address/mask-length vlan-id* **priority** *priority* or use command of **ip-subnet-vlan** *ip-address mask-address vlan-id* or use command of **ip-subnet-vlan** *ip-address/mask-length vlan-id* to configure VLAN based on IP sub-network and at the same time configure corresponding VLAN 802.1p priority of IP sub-network; 3. Done.

Appendix List:

Parameter	Description	Value
ip-address	specify the pursuant source IP address or network address of VLAN divided based on IP sub-network	dotted decimal
mask-address	specify sub-network mask	dotted decimal
vlan-id	specify to divide VLAN ID based on IP sub-network	integer with range of 1~4094
priority	optional, specify corresponding VLAN 802.1p priority of IP address or network segment	integer with range of 0~7, the value is bigger, the priority is higher, default to be 0

2.6.6 Configure VLAN Based on Protocol

Purpose

This section introduces how to configure VLAN divided based on protocol.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step
Configure to divide VLAN based on protocol and specify the associated protocol	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **protocol-vlan** *protocol-index* { **ethernet2** | **snap** } *etransm-typevalue* } or use command of **protocol-vlan** *protocol-index* **llc ssap** { *ssap-value* | **any** } **dsap** { *dsap-value* | **any** } to configure to divide VLAN based on protocol and specify the associated protocol;

Objective	Step
	3. Done.
Configure interface to allow VLAN based on protocol to pass	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter the Interface Configuration View; 3. Use command of **port link-type hybrid** to configure interface link type to be hybrid; 4. Use command of **port hybrid vlan** *vlan-list* **untagged** } to configure Hybrid type interface to join in the VLAN based on protocol; Done.
Configure the associated protocol VLAN of interface	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter the Interface Configuration View; 3. Use command of **protocol-vlan** *protocol-index* **vid** *vlan-id* or use command of **protocol-vlan** *protocol-index* **vid** *vlan-id* **priority** *priority* to configure the associated protocol VLAN of interface; 4. Done.

Appendix List:

Parameter	Description	Value
protocol-index	protocol index value	integer with range of 1~16
ethernet-type-value	divided VLAN based on other protocol type, the protocol type is hex	hex, 0x600~0xffff
ethernet2	specify the encapsulated form of Ethernet message to be Ethernet2	-
snap	specify the encapsulated form of Ethernet message to be snap	-
llc	specify the encapsulated form of Ethernet message to be llc	-
ssap	source service access point	-
dsap	destination service access point	-
any	any service access point	-
ssap-value	source service access point value	hex, 0x01~0xff
dsap-value	destination service access point value	hex, 0x01~0xff
protocol-index	protocol index value	integer with range of 1~16
vlan-id	the associated protocol VLAN ID	integer with range of 1~4094
priority	optional, specify the associated protocol VLAN ID	integer with range of

Parameter	Description	Value
	priority	0~7

2.6.7 Configure VLAN Other Parameters

Purpose

User can choose to use this section operation to configure other VLAN related parameters according to real situation.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step
Configure VLANIF description information	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface vlan** *vlan-id* to create and enter the VLANIF Configuration View; 3. Use command of **description** *description* to configure VLANIF description information; 4. Done.
Configure VLAN description information	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **vlan** *vlan-id1* [*vlan-id2*] to create one or more VLAN and enter the VLAN Configuration View; 3. Use command of **description** *description* to configure VLAN description information; 4. Done.
Modify single VLAN state and VLAN state in batches	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **static-vlan** *vlan-id* to modify single VLAN state and VLAN state in batches; 3. Done.
Configure protocol identification of the current interface outer Tag	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter the Interface Configuration View; 3. Use command of **tpid** { *protocol-id* | **standard** } to configure protocol identification of the current interface outer Tag;Mo 4. Done.
Configure to deal with unknown unicast packet when VLAN forwarding	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **vlan** *vlan-id1* [*vlan-id2*] to create one or more VLAN and enter the VLAN Configuration View; 3. Use command of **unknown-unicast** { **forward** | **drop** } to configure to

Objective	Step
	deal with unknown unicast packet when VLAN forwarding ; 4. Done.
Configure to deal with unknown unicast packet when VLAN forwarding	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **unknown-unicast vlan** *vlan-list* { **forward** | **drop** } or use command of **vlan** *vlan-list* **unknown-unicast** { **forward** | **drop** } or use command of **vlan** *vlan-id* **unknown-unicast** { **forward** | **drop** } to configure to deal with unknown unicast packet when VLAN forwarding ; 3. Done.
Configure the dealing of load sharing mode in trunk interface when VLAN forwarding of aggregation interface	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of unknown-unicast load-balance { dst-mac|src-mac|srcdst-mac|schedule-profile *name* |default } to configure the dealing of load sharing mode in trunk interface when VLAN forwarding of aggregation interface ; 3. Done.
Configure to deal with unknown multicast when VLAN forwarding	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of Use command of **vlan** *vlan-id1* [*vlan-id2*] to create one or more VLAN and enter the VLAN Configuration View; 3. Use command of **unknown-multicast** { **forward** | **drop** } to configure to deal with unknown multicast when VLAN forwarding; 4. Done.
Configure to deal with unknown unicast when VLAN forwarding	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **unknown-multicast vlan** *vlan-list* { **forward** | **drop** } or use command of **vlan** *vlan-list* **unknown-multicast** { **forward** | **drop** } or use command of **vlan** *vlan-id* **unknown-multicast** { **forward** | **drop** } to configure to deal with unknown unicast when VLAN forwarding; 3. Done.
Configure VLAN matching priority of interface	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter the Interface Configuration View; 3. Use command of **vlan precedence** { **mac-vlan** | **ip-subnet-vlan** } to configure VLAN matching priority of interface; 4. Done.
Configure VLAN type to be common VLAN	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface vlan** *vlan-id* to create and enter the VLANIF Configuration View or use command of **vlan** *vlan-id1* [*vlan-id2*] to create one or more VLAN and enter the VLAN Configuration View; 3. Use command of **vlan normal** to configure VLAN type to be common VLAN; 4. Done.

Appendix List:

Parameter	Description	Value
description	specify VLANIF interface description information	character string, not support blank, case sensitive, length range of character string is 1~32
vlan-id	specify the associated protocol VLAN ID	integer with range of 1~4094
protocol-id	the protocol identification of current interface outer Tag	hex, <0x1-0xffff>
standard	standard value	0x8100
schedule-profile	the created enhanced load sharing template mode	-
Name	detailed template name	-
src-mac	specify trunk load sharing based on source MAC address	-
dst-mac	specify trunk load sharing based on destination MAC address	-
srcdst-mac	specify trunk load sharing based on XOR address of source MAC and destination MAC	-
default	default mode	default load sharing mode to be srcdst-mac
mac-vlan	first match VLAN according to the VLAN divided based on MAC	-
ip-subnet-vlan	first match VLAN according to the VLAN divided based on IP sub-network	-

2.6.8 Maintenance and Debug

Purpose

When VLAN function is abnormal, it needs to check and debug.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step
Enable or disable VLAN or VLANIF traffic statistics switch	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface vlan** *vlan-id* to enter the VLANIF Configuration View or use command of **vlan** *vlan-id1* [*vlan-id2*] to create one or more VLAN and enter the VLAN Configuration View;

Objective	Step
	3. Use command of **statistic** { **enable** | **disable** } to enable or disable VLAN or VLANIF traffic statistics switch; 4. Done.
Clear specified VLAN statistics information	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **reset vlan** *vlan-id* **statistic** to clear specified VLAN statistics information; 3. Done.
Check VLAN configuration information divided based on MAC address	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View, Use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter the Interface Configuration View or keep the current Privilege User View; 2. Use command of **show mac-vlan** or use command of **show mac-vlan** *vlan-id* or use command of **show mac-vlan interface** to check VLAN configuration information divided based on MAC address; 3. Done.
Check VLAN configuration information divided based on IP sub-network	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View, Use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter the Interface Configuration View or keep the current Privilege User View; 2. Use command of **show ip-subnet-vlan** or use command of **show ip-subnet-vlan** *vlan-id* or use command of **show ip-subnet-vlan interface** to check VLAN configuration information divided based on IP sub-network; 3. Done.
Check VLAN configuration information divided based on protocol	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View, Use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter the Interface Configuration View or keep the current Privilege User View; 2. Use command of **show protocol-vlan** or use command of **show protocol-vlan** *protocol-index* or use command of **show protocol-vlan interface** to check VLAN configuration information divided based on protocol; 3. Done.
Check VLAN interface configuration information	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface vlan** *vlan-id* to enter the VLANIF Configuration View or keep the current Privilege User View; 2. Use command of **show interface vlan** *vlan-id* **config** or use command

Objective	Step
	of **show interface vlan config** to check VLAN interface configuration information; 3. Done.
Check VLAN related information	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **vlan** *vlan-id* to enter the VLAN Configuration View or use command of **interface vlan** *vlan-id* to enter the VLANIF Configuration View or use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter the Interface Configuration View or keep the current Privilege User View; 2. Use command of **show vlan** or use command of **show vlan all** or use command of **show vlan all** *vlan-list* or use command of **show vlan property** or use command of **show vlan property** *vlan-list* or use command of **show vlan verbose** or use command of **show vlan** *vlan-id* **verbose** to check VLAN related information; 3. Done.
Check VLAN statistics information	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View, Use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter the Interface Configuration View or keep the current Privilege User View; 2. Use command of **show vlan** *vlan-id* **statistic** to check VLAN statistics information; 3. Done.

Appendix List:

Parameter	Description	Value
vlan-id	VLAN ID	integer with range of 1~4094
vlan-list	VLAN list	integer, form as 1,2,3-5

2.6.9 Example

Network Requirement

The development department and market department of enterprise user use SwitchA and SwitchB to connect. It requires that the staff of development department can access Server1 and the staff of market department can access Server2 and the two departments cannot communicate with each other.

- Divide two VLANs separately to be VLAN 100 and VLAN 200 and configure VLAN description to be “Development100” and “Market200”.
- Add computers of development department and Server1 into VLAN100.
- Add computers of market department and Server2 into VLAN200.

Network Topology

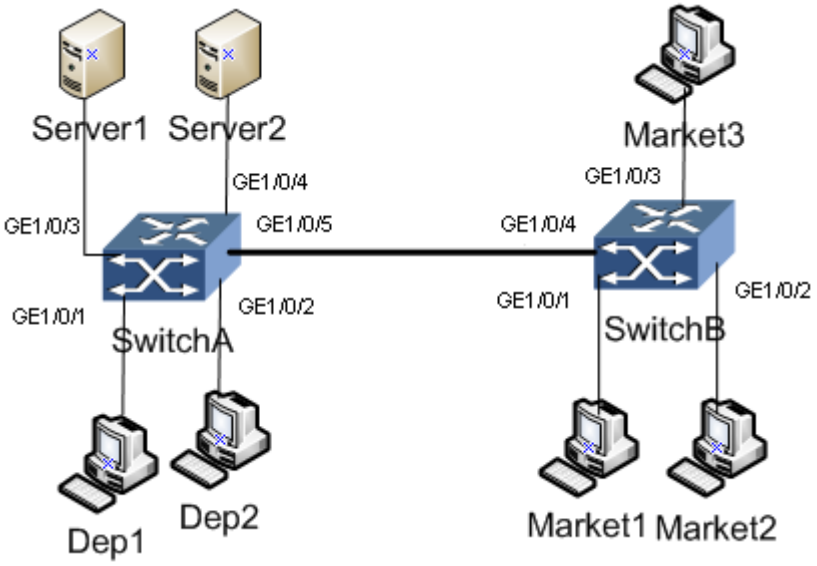


Figure VLAN Configuration Topology

Configuration Step

1. Configure SwitchA.

SwitchA#configure

%Enter configuration commands.End with Ctrl+Z or command “quit” & “end”

//Create VLAN100 and enter its configuration view.

SwitchA(config)#interface vlan 100

SwitchA(config-vlan-100)#

//Confiugre VLAN100 description information to be Development100.

SwitchA(config-vlan-100)#description Development100

//Add interface Ge1/0/1, Ge1/0/2 and Ge1/0/3 into VLAN100 and configure the VLAN100 to be the PVID of interface Ge1/0/1, Ge1/0/2 and Ge1/0/3.

SwitchA(config-vlan-100)#quit

SwitchA(config)#

SwitchA(config)#interface fastethernet 1/0/1

SwitchA(config-ge1/0/1)#port hybrid vlan 100 untagged

SwitchA(config-ge1/0/1)#port hybrid pvid 100

SwitchA(config-ge1/0/1)#quit

SwitchA(config)#interface fastethernet 1/0/2

SwitchA(config-ge1/0/2)#port hybrid vlan 100 untagged

SwitchA(config-ge1/0/2)#port hybrid pvid 100

SwitchA(config-ge1/0/2)#quit

SwitchA(config)#interface fastethernet 1/0/3

SwitchA(config-ge1/0/3)#port hybrid vlan 100 untagged

SwitchA(config-ge1/0/3)#port hybrid pvid 100

SwitchA(config-ge1/0/3)#quit

SwitchA(config)#

//Create VLAN200 and enter its configuration view.

SwitchA(config)#interface vlan 200

SwitchA(config-vlan-200)#

//Configure VLAN200 description information to be Market200.

SwitchA(config-vlan-100)#description Market200

//Add interface Ge1/0/4 and Ge1/0/5 into VLAN100 and configure the VLAN200 to be the PVID of interface Ge1/0/4 and Ge1/0/5.

SwitchA(config-vlan-100)#quit

SwitchA(config)#

SwitchA(config)#interface fastethernet 1/0/4

SwitchA(config-ge1/0/4)#port hybrid vlan 200 untagged

SwitchA(config-ge1/0/4#port hybrid pvid 200

SwitchA(config-ge1/0/4)#quit

SwitchA(config)#interface fastethernet 1/0/5

SwitchA(config-ge1/0/5)#port hybrid vlan 200 tagged

SwitchA(config-ge1/0/5)#port hybrid pvid 200

SwitchA(config-ge1/0/5)#quit

2. Configure SwitchB.

//Create VLAN200 and enter its configuration view.

SwitchB#configure

%Enter configuration commands.End with Ctrl+Z or command “quit” & “end”

SwitchB(config)#interface vlan 202

```
//Configure VLAN200 description information to be Market200.
SwitchB(config-vlan-200)#description  Market200
//Add interface Ge1/0/1, Ge1/0/2, Ge1/0/3 and Ge1/0/4 into VLAN100 and configure the VLAN100 to be the PVID of interface Ge1/0/1, Ge1/0/2 and Ge1/0/3.
SwitchB(config-vlan-100)#quit
SwitchB(config)#
SwitchB(config)#interface fastethernet 1/0/1
SwitchB(config-ge1/0/1)#port hybrid vlan 200 untagged
SwitchB(config-ge1/0/1)#port hybrid pvid 200
SwitchB(config-ge1/0/1)#quit
SwitchB(config)#interface fastethernet 1/0/2
SwitchB(config-ge1/0/2)#port hybrid vlan 200 untagged
SwitchB(config-ge1/0/2)#port hybrid pvid 200
SwitchB(config-ge1/0/2)#quit
SwitchB(config)#interface fastethernet 1/0/3
SwitchB(config-ge1/0/3)#port hybrid vlan 200 untagged
SwitchB(config-ge1/0/3)#port hybrid pvid 200
SwitchB(config-ge1/0/3)#quit
SwitchB(config)#interface fastethernet 1/0/4
SwitchB(config-ge1/0/4)#port hybrid vlan 200 tagged
SwitchB(config-ge1/0/4)#quit
SwitchB(config)#
```

2.7 VLAN Translation Configuration

2.7.1 Bind VLAN Translation Item with Interface

Purpose

This section introduces how to bind VLAN translation item to interface.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step	Parameter

Objective	Step	Parameter
Bind VLAN translation item to interface	1. Use command of configure to enter the Global Configuration View; 2. Use one of the following commands. join translation-vlan map-index { in | out } join translation-vlan map-indexlist { in | out }	Refer to the following table.
Unbind VLAN translation item of interface	1. Use command of configure to enter the Global Configuration View; 2. Use one of the following commands. no join translation-vlan map-index { in | out } no join translation-vlan map-indexlist { in | out }	

Appendix List:

Parameter	Description	Value
map-index	VLAN translation item index	integer with range of 1~768
map-indexlist	multiple VLAN translation item index	integer, form as 1,2,5-10, to be 1~768
in	take effect of ingress direction	-
out	take effect of egress direction	-

2.7.2 Configure or Delete VLAN Translation Item

Purpose

This section introduces how to configure or delete VLAN translation item.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step	Parameter
Delete inner or outer VLAN Tag	1. Use command of to enter the Common User View or the Privilege User View; 2. Use one of the following commands. **translation-vlan** *map-index* **inner-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **delete** { **inner** | **outer** } **[nto1]** **translation-vlan** *map-index* **inner-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **delete** { **inner** | **outer** } **nto1** translation-vlan *map-index* inner-vlan { *vlan-id* | *vlan-id1/vlan-id2* } delete inner delete outer translation-vlan *map-index* inner-vlan { *vlan-id* |	Refer to the following table.

Objective	Step	Parameter
	vlan-id1/vlan-id2 } delete inner delete outer nto1 **translation-vlan** *map-index* **inner-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **delete inner** { **replace** | **add** } **[nto1] outer** *outervlan-id* **translation-vlan** *map-index* **inner-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **delete inner** { **replace** | **add** } **[nto1] outer** *outervlan-id* **priority** *priority* **translation-vlan** *map-index* **inner-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **replace inner** *innervlan-id* **[nto1]** **translation-vlan** *map-index* **inner-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **replace inner** *innervlan-id* **[nto1] priority** *inner-priority* **translation-vlan** *map-index* **inner-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **replace inner** *innervlan-id* **delete outer [nto1]** **translation-vlan** *map-index* **inner-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **replace inner** *innervlan-id* **[nto1] priority** *inner-priority* **delete outer** **translation-vlan** *map-index* **inner-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **replace inner** *innervlan-id* **[nto1]** { **replace** | **add** } **outer** *outervlan-id* **translation-vlan** *map-index* **inner-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **replace inner** *innervlan-id* **[nto1] priority** *inner-priority* { **replace** | **add** } **outer** *outervlan-id* **translation-vlan** *map-index* **inner-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } { **replace** | **add** } **outer** *outervlan-id* **[nto1]** **translation-vlan** *map-index* **inner-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } { **replace** | **add** } **outer** *outervlan-id* **[nto1] priority** *outer-priority* **translation-vlan** *map-index* **inner-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **inner-pri** *priority* **delete** { **inner** | **outer** } **[nto1]** translation-vlan *map-index* inner-vlan { *vlan-id* | *vlan-id1/vlan-id2* } inner-pri *priority* delete inner delete outer [nto1] **translation-vlan** *map-index* **inner-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **inner-pri** *priority* **delete inner** { **replace** | **add** } **outer** *outervlan-id* **[nto1]** **translation-vlan** *map-index* **inner-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **inner-pri** *priority* **delete inner** { **replace** |	

Objective	Step	Parameter
	add } **outer** *outervlan-id* **[nto1] priority** *outer-priority* **translation-vlan** *map-index* **inner-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **inner-pri** *priority* **replace inner** *innervlan-id* **[nto1]** **translation-vlan** *map-index* **inner-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **inner-pri** *priority* **replace inner** *innervlan-id* **[nto1] priority** *inner-priority* **translation-vlan** *map-index* **inner-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **inner-pri** *priority* **replace inner** *innervlan-id* **[nto1] delete outer** **translation-vlan** *map-index* **inner-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **inner-pri** *priority* **replace inner** *innervlan-id* **[nto1] priority** *inner-priority* **delete outer** **translation-vlan** *map-index* **inner-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **inner-pri** *priority* **replace inner** *innervlan-id* **[nto1]** { **replace** | **add** } **outer** *outervlan-id* **translation-vlan** *map-index* **inner-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **inner-pri** *priority* **replace inner** *innervlan-id* **[nto1] priority** *inner-priority* { **replace** | **add** } **outer** *outervlan-id* **translation-vlan** *map-index* **inner-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **inner-pri** *priority* **replace inner** *innervlan-id* { **replace** | **add** } **outer** *outervlan-id* **[nto1] priority** *outer-priority* **translation-vlan** *map-index* **inner-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **inner-pri** *priority* **replace inner** *innervlan-id* **priority** *inner-priority* { **replace** | **add** } **outer** *outervlan-id* **[nto1] priority** *outer-priority* **translation-vlan** *map-index* **inner-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **inner-pri** *priority* { **replace** | **add** } **outer** *outervlan-id* **[nto1]** **translation-vlan** *map-index* **inner-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **inner-pri** *priority* { **replace** | **add** } **outer** *outervlan-id* **priority** *outer-priority* **translation-vlan** *map-index* **inner-vlan** *innervlan-id* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **delete** { **inner** | **outer** } **[nto1]** translation-vlan *map-index* inner-vlan *innervlan-id* outer-vlan { *vlan-id* | *vlan-id1/vlan-id2* } delete inner delete outer [nto1] **translation-vlan** *map-index* **inner-vlan** *innervlan-id*	

Objective	Step	Parameter
	outer-vlan { *vlan-id* | *vlan-id1/vlan-id2* } **delete inner** { **replace** | **add** } **outer** *outervlan-id* **[nto1]** **translation-vlan** *map-index* **inner-vlan** *innervlan-id* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **delete inner** { **replace** | **add** } **outer** *outervlan-id* **[nto1] priority** *outer-priority* **translation-vlan** *map-index* **inner-vlan** *innervlan-id* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **replace inner** *innervlan-id2* **[nto1]** **translation-vlan** *map-index* **inner-vlan** *innervlan-id* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **replace inner** *innervlan-id2* **[nto1] priority** *inner-priority* **translation-vlan** *map-index* **inner-vlan** *innervlan-id* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **replace inner** *innervlan-id2* **delete outer[nto1]** **translation-vlan** *map-index* **inner-vlan** *innervlan-id* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **replace inner** *innervlan-id2* **[nto1] priority** *inner-priority* **delete outer** **translation-vlan** *map-index* **inner-vlan** *innervlan-id* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **replace inner** *innervlan-id2* { **replace** | **add** } **outer** *outervlan-id* **[nto1]** **translation-vlan** *map-index* **inner-vlan** *innervlan-id* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **replace inner** *innervlan-id2* { **replace** | **add** } **outer** *outervlan-id* **[nto1] priority** *outer-priority* **translation-vlan** *map-index* **inner-vlan** *innervlan-id* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **replace inner** *innervlan-id2* **[nto1] priority** *inner-priority* { **replace** | **add** } **outer** *outervlan-id* **translation-vlan** *map-index* **inner-vlan** *innervlan-id* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **replace inner** *innervlan-id2* **[nto1] priority** *inner-priority* { **replace** | **add** } **outer** *outervlan-id* **priority** *outer-priority* **translation-vlan** *map-index* **inner-vlan** *innervlan-id* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } { **replace** | **add** } **outer** *outervlan-id* **[nto1]** **translation-vlan** *map-index* **inner-vlan** *innervlan-id* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } { **replace** | **add** } **outer** *outervlan-id* **[nto1] priority** *outer-priority* translation-vlan *map-index* outer-vlan { *vlan-id* | *vlan-id1/vlan-id2* } delete { inner | outer } [nto1]	

Objective	Step	Parameter
	translation-vlan *map-index* outer-vlan { *vlan-id* | *vlan-id1/vlan-id2* } delete inner delete outer [nto1] **translation-vlan** *map-index* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **delete inner** { **replace** | **add** } **outer** *outervlan-id* **[nto1]** **translation-vlan** *map-index* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **delete inner** { **replace** | **add** } **outer** *outervlan-id* **[nto1] priority** *outer-priority* **translation-vlan** *map-index* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } { **replace** | **add** } **inner** *innervlan-id* **delete outer [nto1]** **translation-vlan** *map-index* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } { **replace** | **add** } **inner** *innervlan-id* **[nto1] priority** *inner-priority* **delete outer** **translation-vlan** *map-index* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } { **replace** | **add** } { **inner** | **outer** } *VLAN-ID* **[nto1]** **translation-vlan** *map-index* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } { **replace** | **add** } { **inner** | **outer** } *VLAN-ID* **[nto1] priority** *priority* **translation-vlan** *map-index* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } { **replace** | **add** } **inner** *innervlan-id* **[nto1]**{ **replace** | **add** } **outer** *outervlan-id* **translation-vlan** *map-index* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } { **replace** | **add** } **inner** *innervlan-id* **[nto1] priority** *inner-priority* { **replace** | **add** } **outer** *outervlan-id* **translation-vlan** *map-index* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } { **replace** | **add** } **inner** *innervlan-id* { **replace** | **add** } **outer** *outervlan-id* **[nto1] priority** *outer-priority* **translation-vlan** *map-index* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } { **replace** | **add** } **inner** *innervlan-id* **[nto1] priority** *inner-priority* { **replace** | **add** } **outer** *outervlan-id* **priority** *outer-priority* translation-vlan *map-index* outer-pri *priority* delete { inner | outer } [nto1] translation-vlan *map-index* outer-pri *priority* delete inner delete outer [nto1] translation-vlan *map-index* outer-pri *priority* delete inner { replace | add } outer *outervlan-id* [nto1]	

Objective	Step	Parameter
	translation-vlan *map-index* outer-pri *priority* delete inner { replace | add } outer *outervlan-id* [nto1] priority *outer-priority* [nto1] translation-vlan *map-index* outer-pri *priority* { replace | add } inner *innervlan-id* delete outer [nto1] translation-vlan *map-index* outer-pri *priority* { replace | add } inner *innervlan-id* priority *inner-priority* delete outer [nto1] translation-vlan *map-index* outer-pri *priority* { replace | add } { inner | outer } *VLAN-ID* [nto1] translation-vlan *map-index* outer-pri *priority* { replace | add } { inner | outer } *VLAN-ID* [nto1] priority *PRIORITY* **translation-vlan** *map-index* **outer-pri** *priority* { **replace** | **add** } **inner** *innervlan-id* **[nto1]**{ **replace** | **add** } **outer** *outervlan-id* **translation-vlan** *map-index* **outer-pri** *priority* { **replace** | **add** } **inner** *innervlan-id* **priority** *inner-priority* **[nto1]**{ **replace** | **add** } **outer** *outervlan-id* **translation-vlan** *map-index* **outer-pri** *priority* { **replace** | **add** } **inner** *innervlan-id* **[nto1]**{ **replace** | **add** } **outer** *outervlan-id* **priority** *outer-priority* **translation-vlan** *map-index* **outer-pri** *priority* { **replace** | **add** } **inner** *innervlan-id* **priority** *inner-priority* **[nto1]** {**replace** | **add** } **outer** *outervlan-id* **priority** *outer-priority* **translation-vlan** *map-index* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **outer-pri** *priority* **delete** { **inner** | **outer** } **[nto1]** translation-vlan *map-index* outer-vlan { *vlan-id* | *vlan-id1/vlan-id2* } outer-pri *priority* delete inner delete outer [nto1] **translation-vlan** *map-index* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **outer-pri** *priority* **delete inner [nto1]** { **replace** | **add** } **outer** *outervlan-id* **translation-vlan** *map-index* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **outer-pri** *priority* **delete inner [nto1]** { **replace** | **add** } **outer** *outervlan-id* **priority** *outer-priority* **translation-vlan** *map-index* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **outer-pri** *priority* { **replace** | **add** } **inner** *innervlan-id* **[nto1] delete outer** translation-vlan *map-index* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **outer-pri** *priority* { **replace** | **add** } **inner**	

Objective	Step	Parameter
	innervlan-id **priority** *inner-priority* **[nto1]delete outer [nto1]** **translation-vlan** *map-index* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **outer-pri** *priority* { **replace** | **add** } { **inner** | **outer** } *VLAN-ID* **[nto1]** **translation-vlan** *map-index* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **outer-pri** *priority* { **replace** | **add** } { **inner** | **outer** } *VLAN-ID* **[nto1] priority** *PRIORITY* **translation-vlan** *map-index* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **outer-pri** *priority* { **replace** | **add** } **inner** *innervlan-id* **[nto1]**{ **replace** | **add** } **outer** *outervlan-id* **[nto1]** **translation-vlan** *map-index* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **outer-pri** *priority* { **replace** | **add** } **inner** *innervlan-id* **priority** *inner-priority* **[nto1]**{ **replace** | **add** } **outer** *outervlan-id* **translation-vlan** *map-index* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } **outer-pri** *priority* { **replace** | **add** } **inner** *innervlan-id* **[nto1]**{ **replace** | **add** } **outer** *outervlan-id* **priority** *outer-priority* **[nto1]** **translation-vlan** *map-index* **outer-vlan** { *vlan-id* | *vlan-id1/vlan-id2* } outer-pri *priority* { **replace** | **add** } **inner** *innervlan-id* **priority** *inner-priority* **[nto1]** { **replace** | **add** } **outer** *outervlan-id* **priority** *outer-priority*	

Appendix List:

Parameter	Description	Value
map-index	VLAN translation item index	integer with range of 1~8192
inner-vlan	matching inner VLAN	-
vlan-id	specify VLAN ID to be matched	integer with range of 1~4094
vlan-id1/vlan-id2	specify VLAN range to be matched, 10/2 means to match all VLAN of VLAN10~VLAN20, vlan-id2 must be more than vlan-id1	integer, vlan-id1 and vlan-id2**,** to be 1~4094
delete	means to delete	-
inner	delete inner VLAN Tag	-
outer	delete outer VLAN Tag	-
delete inner delete outer	delete inner and outer VLAN Tag	-

Parameter	Description	Value
nto1	configure to be n:1 item	-
delete inner	delete inner VLAN Tag	-
{ replace | add } outer	replace outer VLAN Tag or add VLAN Tag	-
outervlan-id	replace or add outer VLAN ID	integer with range of 1~4094
outer-priority	replace or add outer VLAN Tag priority	integer with range of 0~7
priority	outer VLAN Tag priority after being replaced or added	integer with range of 0~7
delete { inner | outer }	delete inner or outer VLAN Tag	-
replace inner	replace inner VLAN Tag	-
innervlan-id	inner VLAN ID after being replaced	integer with range of 1~4094
inner-priority	inner VLAN Tag priority after being replaced	integer with range of 0~7
delete outer	delete outer VLAN Tag	-
delete inner delete outer	delete inner and outer VLAN Tag at the same time	-

2.7.3 Check VLAN Translation Item Related Information

Purpose

This section introduces how to configure the related information of VLAN translation item.

This operation helps user to check the device interface whether to bind VLAN translation item including VLAN translation item index information, ingress binding of interface or egress binding of interface or ingress and egress binding of interface at the same time.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step	Parameter
Check VLAN translation item related information	1. Use command of to enter the Common User View or the Privilege User View; 2. Use one of the following commands. show translation-vlan interface show translation-vlan interface vlan-list show translation-vlan interface all show translation-vlan mapped show translation-vlan mapped vlan-list	vlan-list: VLAN list, optional parameter, support to input multiple VLAN ID. form as 1,3,5-10

2.7.4 Example

Network Requirement

In the access network, family user connects with SwitchA through family gateway and access to the carrier network at last.

Voice service data of User1 is tagged VLAN10 and internet online business data is tagged VLAN11 through the gateway. Internet online business data of User2 is tagged VLAN12 through the gateway.

After passing the SwtichA, the voice service data with VLAN10 of User1 is transmitted to be tagged VLAN100 of carrier operator and the internet online business data with VLAN11 of User1 is transmitted to be tagged VLAN101 of carrier operator. The internet online business data with VLAN12 of User2 is transmitted to be tagged VLAN101.

Network Topology

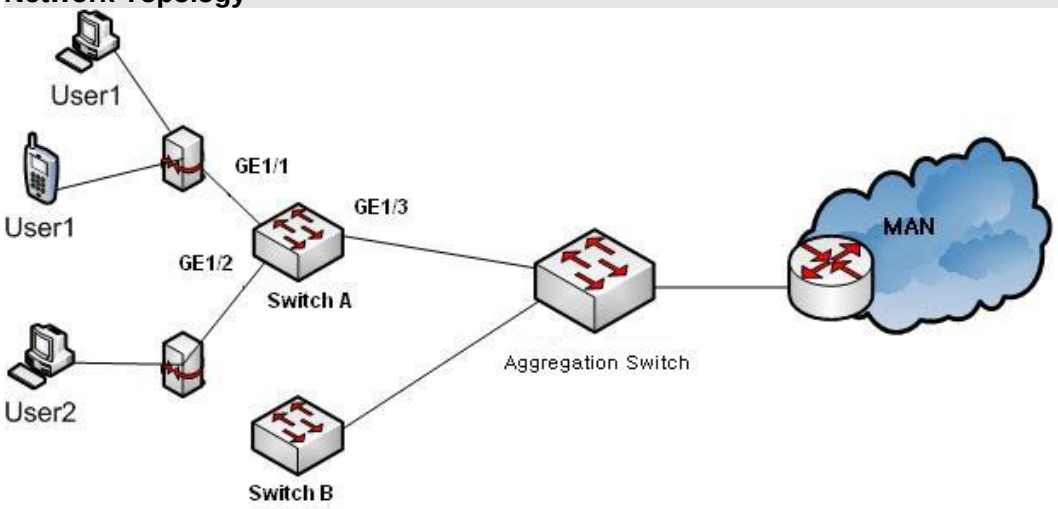


Figure VLAN Translation Configuration Topology

Configuration Step

1. Create user VLAN of access network.
2. Create network carrier operator VLAN.
3. Create VLAN translation rule table.
4. Add the interface connecting with user into the user VLAN and carrier operator VLAN.
5. Add translation rule table on interface.
6. Add the uplink interface into the carrier operator VLAN.

Configure SwitchA.

SwitchA#configure

%Enter configuration commands.End with Ctrl+Z or command “quit” & “end”

//Create user VLAN10, VLAN11 and VLAN12 of access network.

SwitchA(config)#interface vlan 10

SwitchA(config-vlan-10)#quit

SwitchA(config)#interface vlan 11

SwitchA(config-vlan-11)#quit

SwitchA(config)#interface vlan 12

SwitchA(config-vlan-12)#quit

SwitchA(config)#

//Create carrier operator network VLAN100 and VLAN101.

SwitchA(config)#interface vlan 100

SwitchA(config-vlan-100)#quit

SwitchA(config)#interface vlan 101

SwitchA(config-vlan-101)#quit

SwitchA(config)#

//Create VLAN translation rule table: VLAN10->VLAN100, VLAN11->VLAN101 and VLAN12->VLAN101.

SwitchA(config)#

SwitchA(config)# translation-vlan 1 outer-vlan 10 replace outer 100

SwitchA(config)# translation-vlan 2 outer-vlan 11 replace outer 101

SwitchA(config)# translation-vlan 3 outer-vlan 12 replace outer 101

//Enter the GE1/0/1 and add interface into VLAN10, VLAN 11, VLAN100 and VLAN101.

SwitchA(config)#interface fastethernet 1/0/1

SwitchA(config-ge1/0/1)#port hybrid vlan 10 tagged

SwitchA(config-ge1/0/1)#port hybrid vlan 11 tagged

SwitchA(config-ge1/0/1)#port hybrid vlan 100 untagged

SwitchA(config-ge1/0/1)#port hybrid vlan 101 untagged

//Bind VLAN translation item to interface.

SwitchA(config-ge1/0/1)#join translation-vlan 1 in

SwitchA(config-ge1/0/1)#join translation-vlan 2 in

SwitchA(config-ge1/0/1)#quit

//Enter the GE1/0/2 and add interface into VLAN12 and VLAN101.

SwitchA(config)#interface fastethernet 1/0/2

SwitchA(config-ge1/0/2)#port hybrid vlan 12 tagged

SwitchA(config-ge1/0/2)#port hybrid vlan 101 untagged

SwitchA(config-ge1/0/2)# join translation-vlan 3 in

SwitchA(config-ge1/0/2)#quit

SwitchA(config)#

//Create VLAN translation rule table: VLAN101->VLAN10, VLAN101->VLAN11 and VLAN101->VLAN12.

SwitchA(config)#

SwitchA(config)# translation-vlan 1 outer-vlan 100 replace outer 10

SwitchA(config)# translation-vlan 2 outer-vlan 101 replace outer 11

SwitchA(config)#translation-vlan 3 outer-vlan 101 replace outer 12

//Enter the GE1/0/3 and add interface into VLAN10, VLAN 11, VLAN12, VLAN100 and VLAN101.

SwitchA(config)#interface fastethernet 1/0/3

SwitchA(config-ge1/0/3)#port trunk allow-pass vlan 10 untagged

SwitchA(config-ge1/0/3)#port trunk allow-pass vlan 11 untagged

SwitchA(config-ge1/0/3)#port trunk allow-pass vlan 12 untagged

SwitchA(config-ge1/0/3)#port trunk allow-pass vlan 100 tagged

SwitchA(config-ge1/0/3)#port trunk allow-pass vlan 101 tagged

//Bind VLAN translation item to interface.

SwitchA(config-ge1/0/3)#join translation-vlan 1 in

SwitchA(config-ge1/0/3)#join translation-vlan 2 in

SwitchA(config-ge1/0/3)#join translation-vlan 3 in

SwitchA(config-ge1/0/3)#

SwitchA(config-ge1/0/3)#quit

Chapter3
IP Service Configuration

3.1 Summary

This chapter introduces configurations of QSW-2870 Switch IP

services. This chapter includes the following section.

3.2 DHCP Configuration

3.2.1 DHCP Introduction

DHCP Background

The PC connected with Internet needs to know its IP address and other information before sending or receiving data message such as network gateway, sub-network mask and DNS server IP address. PC can obtain the information by BOOTP. BOOTP (Bootstrap Protocol) is a remote boot protocol appearing earlier and it communicates with remote server to obtain necessary information of communication. BOOTP is mainly used for Client without disk to obtain its IP address, IP address of server, boot mapping file name and network gateway IP address from the Server.

BOOTP design is used in relatively static environment. Each host has a permanent network connection. Administrator creates a BOOTP configuration file and this file defines a group of BOOTP parameters for each host. Because the configuration usually remains unchanged, this file will not change usually. The configuration usually remains unchanged for weeks typically.

With the unceasing expansion of network scale and the increasing complexity of network, the case that the computer number is more than the number of available IP address usually appears. At the same time, with the wide use of portable computer and wireless network, the location of computer usually changes and the corresponding IP address should be usually updated. This make the network

configuration more complicated. DHCP (Dynamic Host Configuration Protocol) is developed to meet these commands. DHCP uses Client/Server communication mode. Client applies configuration to Server and Server returns the IP address and such corresponding information to realize dynamic configuration of IP address and other information like this.

DHCP Related Terms

- DHCP Server

  The supplier of DHCP service interacts with DHCP Client by using DHCP message. It distributes appropriate IP address for various types of Clients and distributes other network parameters according to the requirements.

- DHCP Client

  DHCP Client is the trigger and driver of the whole DHCP process. It communicates with DHCP Server by using DHCP message to obtain IP address and other network parameters.

- DHCP Relay

  DHCP Relay is the relay transmitter of DHCP message. It is between the DHCP Client and Server of different network segment to assume the relay service. And it solves the problem that DHCP Client and DHCP Server must be in the same network segment.

- DHCP Snooping

  DHCP Snooping is the layer two monitoring function of DHCP service. Using this function can record user IP address and MAC address.

DHCP General Options

In order to be compatible with BOOTP, DHCP reserves the message format of BOOTP. The difference of DHCP and BOOTP message is mainly reflected in the Option field. The increased function of DHCP based on BOOTP is achieved by Option field.

DHCP uses Option filed to transmit control information and network configuration parameter to realize dynamic distribution of address and provides more abundant network configuration information for Client.

Common DHCP Options:

- Option 3: router option used to specify the distributed network gateway network for Client.
- Option 6: DNS Server option used to specify the distributed DNS Server address for Client.
- Option 51: IP address lease option.
- Option 53: DHCP message type option used to identify DHCP message type.
- Option 55: request parameter list. Client uses this option to specify to obtain which network configuration parameters from Server. This option content is the value corresponding with the parameters required by Client.
- Option 66: TFTP Server name option used to specify the distributed TFTP Server domain name for Client.
- Option 67: starting file name option used to specify the distributed starting file name for Client.
- Option 150: TFTP Server address option used to specify the distributed TFTP Server address for Client.
- Option 121: non-classification routing option. This option includes a group of non-classification static routing (the mask of destination address is any value and can divide sub-network by mask). After Client receives this option, Client will add these static routing in routing table.
- Option 33: static routing option. This option includes a group of classified static routing (the mask of destination address is fixed to be a natural mask and cannot divide sub-network). After Client receives this option, Client will add these static routing in routing table. If Option121 exists, this option will be ignored.

More DHCP option introduction refers to RFC 2132.

DHCP Advantages and Disadvantages

DHCP uses Client/Server communication mode. All IP network configuration parameters are managed by DHCP Server concentrated and DHCP Server is responsible for dealing with the DHCP request of Client. Client will use the IP network parameter distributed by Server to communicate.

According to the different requirements of Client, DHCP provides three types of IP address distribution policy. Administrator can choose DHCP to use which policy to response to every network or each host.

- Distribute Address Manually: statically bind fixed IP address by administrator for a few of specified Clients (such as WWW Server). DHCP sends the configured and fixed IP address to Client.
- Distribute Address Automatically: DHCP distributes the IP address with infinite lease for Client.
- Distribute Address Dynamically: DHCP distributes the IP address with period of validity for Client. Reaching the period of validity, Client needs to apply for address again.

DHCP expands the BOOTP from the following two aspects.

- DHCP allows computer to obtain IP address fast and dynamically. In order to use the DHCP dynamic address distribution mechanism, administrator must configure DHCP Server and make DHCP Server offer a group of IP addresses called address pool. Once new computer connects with network in any time, this computer will communicate with Server and apply for an IP address. Server chooses an address from the configured address pool and distributes it to this computer.
- Compared with BOOTP, DHCP can provide more abundant network configuration information for Client.

DHCP has the following disadvantages.

- When there are multiple DHCP Servers in the network, one DHCP Server cannot find out the IP address which has been leased by other Server.
- DHCP Server cannot communicate with Client in different network segment unless the message is forwarded by DHCP Relay.

 Attention:

- Only after enabling DHCP Relay, DHCP Option82 function can take effective.

- It suggests to use DHCP Option 82 function on the device most closing to the DHCP Client in order to precisely orientate the user location.

3.2.2 DHCP Server

DHCP Server Application Environment

In the following situation, DHCP Server is usually used to achieve the IP address distribution.

- Network scale is large and manual configuration requires a log of work and it is hard to manage the whole network centrally.
- The number of host in network is greater than the number of supported IP address in network. It cannot distribute a fixed IP address for every host and limit the number of user accessing the network (for example, Interface access service provider is this case). Most users must obtain IP address dynamically by DHCP Server.
- Only a few hosts in network need fixed IP address and most hosts do not have this command of fixed IP address.

DHCP Server Address Management

DHCP Server chooses and distributes IP address and other related parameters from the address pool. When the device used as the DHCP Server receives the DHCP request from Client, it will choose appropriate address pool according to configuration and choose a free IP address from the address pool. The device will send the free address with other related parameters (DNS Server address, address lease period) to Client.

DHCP Server Security Function

- Fake Server Detection Function

  In network, if there is DHCP Server secretly set up, when other users apply IP address, this DHCP Server will communicate with DHCP Client and result in wrong IP address obtained by user and the user cannot access the network normally. This kind of DHCP Server is called fake DHCP Server.

  After enabling fake DHCP Server detection function on DHCP Server, when DHCP Client sends DHCP-REQUEST message, DHCP Server will obtain the IP

address of Server which distributes IP address to Client and record this IP address and information of interface receiving the message so as to discover and deal with Fake DHCP Server in time for administrator.

- IP Address Repeated Detection Function

  In order to prevent repeated IP address allocation resulting in address conflict, before DHCP Server allocates IP address for DHCP Client, it needs to detect this IP address.

  Using Ping function to realize address detection. It judges whether there is address conflict by testing whether DHCP Server can get the Ping response within the specified time. The designation address sent by DHCP Server is the ICMP message with address to be allocated. If it does not receive response within specified time, it will continue to send ICMP message until the Ping operation time reaches the maximum. If it still does not get response, it will allocate address to Client so as to assure that the IP address allocated to Client is unique.

- Address Matching Detection Function (Anti-static IP User Function)

  When DHCP Server allocates IP address to user, it will record the binding relationship of IP address and MAC address. User can also configure user address table manually (that is static binding of IP address and MAC address). In order to prevent illegal user from configuring a static IP address and access other network, if the corresponding relationship of IP address and MAC address configured by user does not exist in the user address table of DHCP Server (include the DHCP table dynamically recorded and user address table manually configured), DHCP Server will not allow user to access network outside. This function only takes effect when DHCP Client and DHCP Server are in the same network segment.

3.2.3 DHCP Relay

DHCP Relay Application Environment

The original DHCP protocol requires that Client and Server must be in the same network segment and cannot work across network segments. In order to configure host dynamically, it needs to configure a DHCP Server in all network segments and

this is not economical. DHCP Relay solves this problem. It provides relay service between DHCP Client and DHCP Server in different network segment and sends DHCP message to DHCP Server across network segment. So DHCP Client of different network can use the same DHCP Server. And this saves cost and also facilitate the centralized management.

DHCP Relay is between DHCP Client and DHCP Server of different network segment and it provides relay service for DHCP Client and DHCP Server.

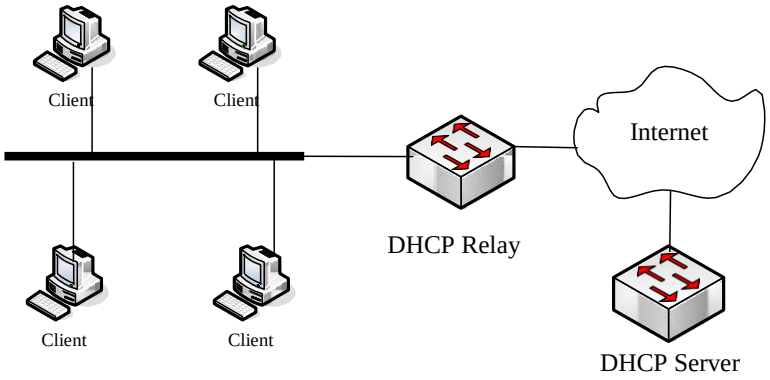


Figure DHCP Application Environment Topology

Option82 Supported by DHCP Relay

When DHCP Server and DHCP Client are not in the same sub-network, if Client wants to be allocated IP address from DHCP Server, DHCP Relay Agent must be used to forward DHCP request packet. Before DHCP Relay Agent sends the DHCP message of Client to DHCP Server, it can insert some option information so that the DHCP Server can get Client information precisely and allocate IP address and other parameters flexibly according to corresponding policy. This option is called to be DHCP relay agent information option and option number is 82. So it also called to be option 82 and related standard document is RFC3046.

Option 82 is the expanded application of DHCP option. Option82 is only a application expansion, it will not influence the DHCP original application whether carrying option82 or not. DHCP Server not supporting option82 receives the message inserted option82 or DHCP Server supporting option82 receives message without option82, these two cases do not influence the original basic DHCP service. If want to support

the expansion application of option82, DHCP Server itself must support option82 and the message received must be inserted option82 information.

Option82 can identify different users and Server can allocate different IP address for different users according to option82 so as to realize QoS, security and accounting management.

DHCP Relay Security Function

- Address Matching Detection Function

  When DHCP Client obtains IP address from DHCP Server by DHCP Relay, DHCP Relay will record the binding relationship of IP address and MAC address. User can also configure user address table item manually (static binding of IP address and MAC address). In order to prevent illegal user from configuring an IP address statically and accessing other network, device supports address matching check function of DHCP Relay. When enabling this function on device, if the corresponding relationship of user configured IP address and user MAC address is not in the user address table of DHCP Relay (including the dynamically recorded table of DHCP Relay and manually configured user address table item), then DHCP Relay will not allow this user to access network outside.

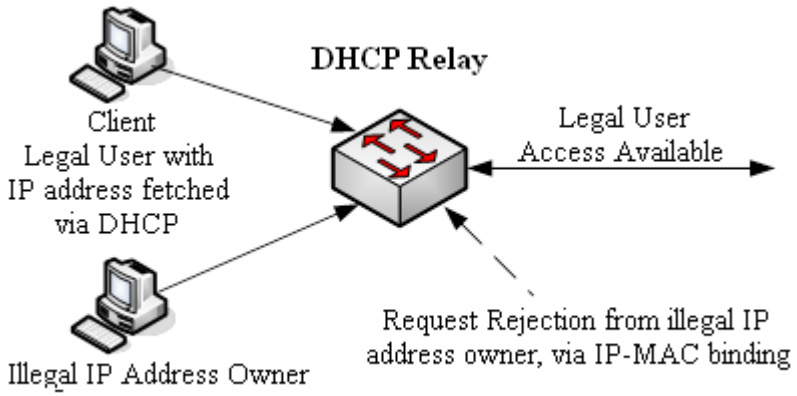


Figure DHCP Security Topology

- User Table Timing Updating Function

When DHCP Client obtains IP address from DHCP Server by DHCP Relay, DHCP Relay will record the binding relationship of IP address and MAC address. When DHCP Client releases this IP address, DHCP Client will send unicast DHCP-RELEASE message to DHCP Server and DHCP Relay will not deal with this message, it will result in that the user address item of DHCP Relay will not be updated in real time. User can configure the timing updating function of DHCP Relay dynamic user table item to solve the problem above.

Every other specified time, DHCP Relay sends DHCP-REQUEST message to DHCP Server with IP address allocated to DHCP Client and its own MAC address.

If DHCP Server responds to DHCP-ACK message, it means that this IP address can be allocated and DHCP Relay will age the corresponding table item in dynamic user address table.

If DHCP Server responds to DHCP-NAK message, it means that this IP address lease still exists and DHCP Relay will not age this IP address table item.

- Fake Server Detection Function

  In network, if there is DHCP Server secretly set up, when other users apply IP address, this DHCP Server will communicate with DHCP Client and result in wrong IP address obtained by user and the user cannot access the network normally. This kind of DHCP Server is called fake DHCP Server.

  After enabling Fake DHCP Server detection function on DHCP Relay, when DHCP-REQUEST message, DHCP Relay will obtain the IP address of Server which distributes IP address to Client and record this IP address and information of interface receiving the message so as to discover and deal with Fake DHCP Server in time for administrator.

3.2.4 Configure DHCP Server

Precondition

Please make sure that DHCP Client can communicate with QSW-2870 normally.

Purpose

Configure DHCP Server to finish IP address assignation.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step
Globally enable DHCP function	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **dhcp start** to globally enable DHCP function; 3. Done.
Configure DHCP working mode of interface to be Server	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface vlan** *vlan-id* to enter the VLANIF Configuration View; 3. Use command of **ip dhcp server** to configure DHCP working mode of interface to be Server; 4. Done.
Configure DHCP address pool	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **dhcp pool** *pool-number* to create DHCP address pool and enter the DHCP pool Configuration View; 3. Done.
Configure DHCP dynamic distributed IP address range and mask in the address pool	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **dhcp pool** *pool-number* to enter the DHCP pool Configuration View; 3. Use command of **network range** *start-ip-address end- ip-address* **mask** *mask-address* or use command of **network** *ip-address* **mask** *mask-address* to configure DHCP dynamic distributed IP address range and mask in the address pool; 4. Done.
(Optional) Configure the IP address not automatically assigned in DHCP address pool	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **dhcp pool** *pool-number* to enter the DHCP pool Configuration View; 3. Use command of **dhcp server forbidden-ip** *ip-address1* [*ip-address2*] to Configure the IP address not automatically assigned in DHCP address pool; 4. Done.
Configure the IP address lease time in DHCP address pool	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **dhcp pool** *pool-number* to enter the DHCP pool Configuration View; 3. Use command of **lease-time** { *time* | **default** } to configure the IP address lease time in DHCP address pool; 4. Done.
Configure the	1. Use command of **configure** to enter the Global Configuration View;

Objective	Step
network gateway IP address for DHCP Client assigned by DHCP address pool	2. Use command of **dhcp pool** *pool-number* to enter the DHCP pool Configuration View; 3. Use command of **gateway** *ip-address* to configure the network gateway IP address for DHCP Client assigned by DHCP address pool; 4. Done.
(Optional) Configure the IP address of DNS server	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **dhcp pool** *pool-number* to enter the DHCP pool Configuration View; 3. Use command of **dns** *ip-address* or use command of **dns** *ip-address* **backup** to configure the IP address of DNS server; 4. Done.

Appendix List:

Parameter	Description	Value
vlan-id	VLAN ID	integer with range of 1~4094
pool-number	address pool number	integer with range of 1~64
start-ip-address	the starting IP address	dotted decimal
end- ip-address	the ending IP address	dotted decimal
mask-address	mask address	dotted decimal
ip-address	network address	dotted decimal
ip-address1	the minimum IP address not automatically assigned	dotted decimal
[ip-address2]	the maximum IP address not automatically assigned, must not be less than ip-address1. If not designate this parameter, there is only one IP address.	dotted decimal
time	valid time for lease	integer with range of 1~120, unit:hour
default	default valid lease time	24 hours
ip-address	network gateway IP address	dotted decimal
ip-address	DNS or backup DNS IP address	dotted decimal

3.2.5 Configure DHCP Server Supported Option

Precondition

DCHP Server has been configured already.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step
Configure the user defined option value of DHCP	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **dhcp pool** *pool-number* to enter the DHCP pool Configuration View; 3. Use command of **dhcp option** *option1-range* **ip-address** *ip-address* or use command of **dhcp option** *option2-range* **ascii** *ascii-string* or use command of **dhcp option** *option3-range* **hex** *hex-string* to configure the user defined option value of DHCP; 4. Done.
Configure the hex value of option212	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **dhcp pool** *pool-number* to enter the DHCP pool Configuration View; 3. Use command of **dhcp option 6rd ipv4 prefix-len** *len-range* **prefix** *ipv6-address/MASK* **br** *ivp4-address* to configure the hex value of option212; 4. Done.
Configure the sub-option attribute value of DHCP user defined option	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **dhcp pool** *pool-number* to enter the DHCP pool Configuration View; 3. Use command of **dhcp option** *option-range* **sub-option** *sub-option* **ip-address** *ip-address* or use command of **dhcp option** *option-range* **sub-option** *sub-option* **ascii** *ascii-string* or use command of **dhcp option** *option-range* **sub-option** *sub-option* **hex** *hex-string* to configure the sub-option attribute value of DHCP user defined option; 4. Done.

Appendix List:

Parameter	Description	Value
option1-range	option range	integer with range of 2-254
option2-range	option range	integer with range of 2-254
option3-range	option range	integer with range of 2-254
ip-address	designate option60 to be IP address type	dotted decimal
ascii-string	designate option60 to be ASCII character string type	character string, length to be 1~255
hex-string	designate option60 to be hex type	the inputted character string

Parameter	Description	Value
		must be even number, hex (such as HH or HHHH)
len-range	IP address mask length	integer with range of 0-32
ipv6-address/MAS	IPv6 address prefix and prefix length	128bits IP address is divided into 8 groups, 16bits of each group uses 4 hex characters (0 ～ 9, A ～ F), use colon to separate groups
option-range	option range	integer with range of 2-254
sub-option	sub-option range	integer with range of 1-254
ip-address	IPv4 address of sub-option	dotted decimal

3.2.6 Configure DHCP Server Security Function

Precondition

DCHP Server has been configured already.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step
Bind IP address of DHCP address pool with user MAC address	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **dhcp server static-bind** *ip-address mac-address* to bind IP address of DHCP address pool with user MAC address; 3. Done.
Configure the address repeated detection interval	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **dhcp address-check-time** { *checktime* | **default** } to configure the address repeated detection interval; 3. Done.
Configure DHCP fake server detection function	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **dhcp server detect** { **enable** | **disable** } to configure DHCP fake server detection function; 3. Done.

Appendix List:

Parameter	Description	Value
ip-address	the binding IP address must be the valid IP address in the address	dotted decimal

Parameter	Description	Value
	pool	
mac-address	user MAC address	form as AA:BB:CC:DD:EE:FF, A~F is one hex
checktime	the maximum time of address conflict detection	integer with range of 0~10000, unit: millisecond
default	default value	500, unit: millisecond

3.2.7 Configure DHCP Relay

Purpose

Configure DHCP relay to realize IP address assigned to user of DHCP Server crossing network.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step
Globally enable DHCP function	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **dhcp start** to globally enable DHCP function; 3. Done.
Configure DHCP interface to work in Relay mode	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface vlan** *vlan-id* to enter the VLANIF Configuration View; 3. Use command of **ip dhcp relay** to configure DHCP interface to work in Relay mode; 4. Done.
Configure the DHCP server IP address of DHCP relay agent	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface vlan** *vlan-id* to enter the VLANIF Configuration View; 3. Use command of **dhcp relay server-ip** *ip-address* to configure the DHCP server IP address of DHCP relay agent; 4. Done.
(Optional) Enable or disable DHCP relay to support option82 function	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface vlan** *vlan-id* to enter the VLANIF Configuration View; 3. Use command of **dhcp option82** { **enable** | **disable** } to enable or disable DHCP relay to support option82 function; 4. Done.

Objective	Step
(Optional) Configure the dealing policy for the request message sent by DHCP Client with option82 of DHCP relay	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface vlan** *vlan-id* to enter the VLANIF Configuration View; 3. Use command of **dhcp option82** { **drop** | **keep** | **replace** } to configure the dealing policy for the request message sent by DHCP Client with option82 of DHCP relay; 4. Done.
(Optional) Configure the Circuit ID of DHCP Option82	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface vlan** *vlan-id* to enter the VLANIF Configuration View; 3. Use command of **dhcp option82 circuit-id** *circuited* to configure the Circuit ID of DHCP Option82 4. Done.
(Optional) Configure the Remote ID of DHCP Option82	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface vlan** *vlan-id* to enter the VLANIF Configuration View; 3. Use command of **dhcp option82 remote-id** *remoteid* to configure the Remote ID of DHCP Option82; 4. Done.
(Optional) Configure the static user address binding table of DHCP relay	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **dhcp relay static-bind** *ip-address mac-address* to configure the static user address binding table of DHCP relay; 3. Done.
(Optional) Confiugre the timing updating period of DHCP relay user table	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **dhcp relay user refresh-interval** { *interval* | **default** } to Confiugre the timing updating period of DHCP relay user table ; 3. Done.
(Optional) Configure DHCP address matching detection function	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface vlan** *vlan-id* to enter the VLANIF Configuration View; 3. Use command of **dhcp address-check** { **enable** | **disable** } to Configure DHCP address matching detection function; 4. Done.
(Optional) Configure DHCP fake server detection function	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **dhcp server detect** { **enable** | **disable** } to configure DHCP fake server detection function; 3. Done.

Appendix List:

Parameter	Description	Value
vlan-id	VLAN ID	integer with range of 1~4094
ip-address	the DHCP server IP address of DHCP relay agent	dotted decimal
drop	If message has the Option82, then drop this message.	-
keep	If message has the Option82, then keep the Option82 content unchanged and transmit it.	-
replace	If message has the Option82, then replace the original Option82 of the message	-
circuitid	sub-option of DHCP relay, circuit ID	character string
remoteid	user defined remote ID sub-option content Remote ID includes device MAC address default. If using command to configure this sub-option content, then the Remote ID of option82 is the content configure.	character string, case sensitive
ip-address	DHCP Client IP address	dotted decimal
mac-address	DHCP Client MAC address	form as AA:BB:CC:DD:EE:FF, A~F is one hex number
interval	the timing updating period of DHCP relay user table	integer with range of 60~3600, unit: second
default	default value of the timing updating period of DHCP relay user table	1800s

3.2.8 Maintenance and Debug

Purpose

When DHCP function is abnormal, it can use this section operation to check and debug.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step
Enable DHCP Relay debug function	1. Keep the current Privilege User View; 2. Use command of **debug dhcp relay** to enable DHCP Relay debug function;

Objective	Step
	3. Done.
Enable DHCP server debug function	1. Keep the current Privilege User View; 2. Use command of **debug dhcp server** to enable DHCP server debug function; 3. Done.
Enable DHCP fake-server debug function	1. Keep the current Privilege User View; 2. Use command of **debug dhcp fake-server** to enable DHCP fake-server debug function; 3. Done.
Clear DHCP relay statistics information	1. Keep the current Privilege User View; 2. Use command of **reset dhcp relay statistic** to clear DHCP relay statistics information; 3. Done.
Clear DHCP server statistics information	1. Keep the current Privilege User View; 2. Use command of **reset dhcp server statistic** to clear DHCP server statistics information; 3. Done.
Check device DHCP related parameters configuration state information	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface vlan** *vlan-id* to enter the VLANIF Configuration View or keep the current Privilege User View; 2. Use command of **show dhcp** to check device DHCP related parameters configuration state information; 3. Done.
Check device DHCP configuration information	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface vlan** *vlan-id* to enter the VLANIF Configuration View or keep the current Privilege User View; 2. Use command of **show dhcp config** to check device DHCP configuration information; 3. Done.
Check device DHCP user table information	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface vlan** *vlan-id* to enter the VLANIF Configuration View or keep the current Privilege User View; 2. Use command of **show dhcp bind-entry** to check device DHCP user table information; 3. Done.
Check IP address lease	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use

Objective	Step
management information of address pool	command of **interface vlan** *vlan-id* to enter the VLANIF Configuration View or keep the current Privilege User View; 2. Use command of **show dhcp lease-entry** to check IP address lease management information of address pool; 3. Done.
Check device all DHCP address pool configuration information	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface vlan** *vlan-id* to enter the VLANIF Configuration View or keep the current Privilege User View; 2. Use command of **show dhcp pool** to check device all DHCP address pool configuration information; 3. Done.
Check DHCP Relay server configuration information	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface vlan** *vlan-id* to enter the VLANIF Configuration View or keep the current Privilege User View; 2. Use command of **show dhcp relay** to check DHCP Relay server configuration information; 3. Done.
Check DHCP Relay statistics information	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface vlan** *vlan-id* to enter the VLANIF Configuration View or keep the current Privilege User View; 2. Use command of **show dhcp relay statistic** to check DHCP Relay statistics information; 3. Done.
Check user table information of DHCP Relay (including dynamic and static information)	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface vlan** *vlan-id* to enter the VLANIF Configuration View or keep the current Privilege User View; 2. Use command of **show dhcp relay user** to check user table information of DHCP Relay; 3. Done.
Check DHCP Server configuration information	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface vlan** *vlan-id* to enter the VLANIF Configuration View or keep the current Privilege User View; 2. Use command of **show dhcp server** to Check DHCP Server configuration information; 3. Done.

Objective	Step
Check DHCP Server address conflict statistics information	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface vlan** *vlan-id* to enter the VLANIF Configuration View or keep the current Privilege User View; 2. Use command of **show dhcp server conflict** to check DHCP Server address conflict statistics information; 3. Done.
Check DHCP Server timeout information	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface vlan** *vlan-id* to enter the VLANIF Configuration View or keep the current Privilege User View; 2. Use command of **show dhcp server expired** to check DHCP Server timeout information; 3. Done.
Check DHCP Server statistics information	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface vlan** *vlan-id* to enter the VLANIF Configuration View or keep the current Privilege User View; 2. Use command of **show dhcp server statistic** to check DHCP Server statistics information; 3. Done.
Check the DHCP related configuration information of some VLAN interface	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface vlan** *vlan-id* to enter the VLANIF Configuration View or keep the current Privilege User View; 2. Use command of **show dhcp vlan** vlan-id **config** to check the DHCP related configuration information of some VLAN interface ; 3. Done.

Appendix List:

Parameter	Description	Value
vlan-id	VLAN ID	integer with range of 1~4094

3.2.9 Example

Network Requirement

DHCP Server assigns IP address dynamically for clients of different network segment. The network segments of user are 10.1.1.0/24 and 10.1.2.1/24.

The detailed requirements are as follows.

- The address lease time of 10.1.1.0/24 network segment is 12 hours. DNS Server IP address is 10.1.1.200 and egress network gateway address is 10.1.1.1.
- The address lease time of 10.1.2.0/24 network segment is 24 hours. DNS Server IP address is 10.1.2.200 and egress network gateway is 10.1.2.1.

Network Topology

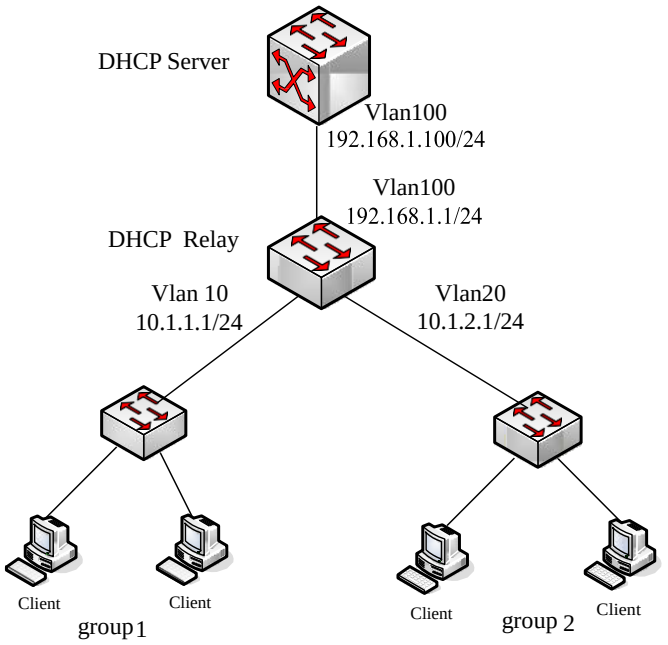


Figure DHCP Configuration Topology

Configuration Step

1. **Configure DHCP Server.**

//Configure VLAN-interface100 IP address of DHCP Server.

Switch#configure

Switch(config)#dhcp enable

Switch(config)#interface vlan 100

Switch(config-vlan-100)#ip address 192.168.1.100/24

Switch(config-vlan-100)#ip dhcp server

//Configure address pool1: address pool range, lease time and designate DNS server.

Switch(config)#dhcp pool 1

Switch(config-dhcp-pool-1)#network range 10.1.1.2 10.1.1.100 mask 255.255.255.0

Switch(config-dhcp-pool-1)#gateway 10.1.1.1

Switch(config-dhcp-pool-1)#lease-time 12

Switch(config-dhcp-pool-1)# dns 10.1.1.200

//Configure address pool2: address pool range, lease time and designate DNS server.

Switch(config)#dhcp pool 2

Switch(config-dhcp-pool-2)#network range 10.1.2.2 10.1.2.100 mask 255.255.255.0

Switch(config-dhcp-pool-2)#gateway 10.1.2.1

Switch(config-dhcp-pool-2)#lease-time 24

Switch(config-dhcp-pool-2)# dns 10.1.2.200

2. Configure DHCP Relay.

//Configure VLAN-interface10 IP address of DHCP Relay and configure to be the Relay mode.

Switch#configure

Switch(config)#dhcp enable

Switch(config)#interface vlan 10

Switch(config-vlan-10)#ip address10.1.1.1/24

Switch(config-vlan-10)#ip dhcp relay

Switch(config-vlan-10)#dhcp relay server-ip 192.168.1.100

//Configure VLAN-interface20 IP address of DHCP Relay and configure to be the Relay mode.

Switch#configure

Switch(config)#interface vlan 20

Switch(config-vlan-20)#ip address 10.1.2.1/24

Switch(config-vlan-20)#ip dhcp relay

Switch(config-vlan-20)#dhcp relay server-ip 192.168.1.100

//Configure VLAN-interface100 IP address of DHCP Relay and configure to be the Relay mode.

Switch#configure

Switch(config)#interface vlan 100

Switch(config-vlan-100)#ip address 1.1.1.1/24

Switch(config-vlan-100)#ip dhcp relay

Chapter4 Routing Configuration

4.1 Summary

This chapter introduces configurations of QSW-2870 Switch routing function, including its background, basic configuration process and configuration examples.

This chapter includes the following section.

4.2 Static Routing Configuration

4.2.1 Static Routing Introduction

Static routing is a particular routing mechanism that requires configuration in manual by the administrator.

When the network structure is simple, static routing can be qualified enough to deploy so that to make the network working normally. The static routing is able to improve network performance as well as guarantee bandwidth for important applications.

The disadvantage of static routing is that once there is failure or fault occurs in the network, the static routing cannot change accordingly and automatically, the intervention from the network administrator is required.

4.2.2 Configure Static Routing

Purpose

This section introduces how to provision static routing information of IPv4 and IPv6.

Process

According to the different purposes, execute corresponding step. Please refer to the following table.

Purpose	Step	Parameter Description

Purpose	Step	Parameter Description
Configure an IPv4 static route	1. Use command of **configure** to access global configuration view; 2. Use command of **ip route-static** *ip-address mask-address nexthop-address* or **ip route-static** *ip-address mask-address nexthop-address NAME* or **ip route-static** *ip-address mask-address nexthop-address metric <0-255>* to configure an IPv4 static route; 3. Done.	In default, system has no static routing list
Delete IPv4 static route	1. Use command of **configure** to access global configuration view; 2. Use command of **no ip route-static** *ip-address mask-address* or **no ip route-static** *ip-address mask-address nexthop-address* or **no ip route-static all** to delete IPv4 static route; 3. Done.	
Configure an IPv6 static route	1. Use command of **configure** to access global configuration view; 2. Use command of **ipv6 route-static** *ipv6-address mask-length ipv6- nexthop-address* **VLAN** *VLAN ID* to configure an IPv6 static route; 3. Done.	
Delete IPv6 static route	1. Use command of **configure** to access global configuration view; 2. Use command of **no ipv6 route-static** *ipv6-address mask-length* to delete IPv6 static route; or **no ipv6 route-static all** to delete all IPv6 static routes; 3. Done.	
Enable or disable IPv6 unicast forwarding	1. Use command of **configure** to access global configuration view; 2. Use command of **ipv6 unicast-forwarding** { **enable | disable** } to enable or disable IPv6 unicast forwarding; 3. Done.	
Configure IPv6 hop limit	1. Use command of **configure** to access global configuration view; 2. Use command of **ipv6 hop-limit** *hop-limit numbe* to configure IPv6 hop limit;	

Purpose	Step	Parameter Description
	3. Done.	

Appended List:

Parameter	Description	Value
ip-address	Destination IP address	Dotted decimal form, e.g., (A.B.C.D, where A~D is decimal number from 0~255).
mask-address	Mask of destination IP address	Dotted decimal form, e.g., (A.B.C.D, where A~D is decimal number from 0~255).
nexthop-address	Designated next hop IP address of the route	Dotted decimal form, e.g., (A.B.C.D, where A~D is decimal number from 0~255).
NAME	Route name defined to a certain route	-
metric <0-255>	Route metric value	Integer form with range of 0~255.
ipv6-address	Destination IPv6 address	Pure binary numbers indication: 128 0s and 1s with 16 bits each group and 8 group in total
mask- length	Mask length of destination IP address	Integer form with range of 0~128.
ipv6-nexthop-address	Designated next hop IPv6 address of the rout	Dotted decimal form, e.g., (A.B.C.D, where A~D is decimal number from 0~255).
VLAN ID	VLAN name	Integer form with range of 1~4094.
hop-limit number	Hop limit of IPv6	Integer form with range of 0~255.

4.2.3 Maintenance and Debug

Purpose

The operation in this section is for situation when static route works abnormal and requires function check, debug and defection orientation.

Process

According to the different purposes, execute corresponding step. Please refer to the following table.

Purpose	Step
Check IP config file information	1. Use command of **disable** to quit back to regular user view or use command of **configure** to access global configuration view, or no command executed to remain in current privilege user view; 2. Use command of **show ip config** to display IP config file information; 3. Done.
Check route information	1. Use command of **disable** to quit back to regular user view or use command of **configure** to access global configuration view, or no command executed to remain in current privilege user view; 2. Use command of **show ip route** or **show ip route** *ip-address* to display routing information; 3. Done.
Check IPv4/IPv6 statistic information of routing table	1. Use command of **disable** to quit back to regular user view or use command of **configure** to access global configuration view, or no command executed to remain in current privilege user view; 2. Use command of **show** { **ip** | **ipv6**} **routing-table statistic** to display IPv4/IPv6 statistic information of routing table; 3. Done.
Check IPv6 interface information	1. Use command of **disable** to quit back to regular user view or use command of **configure** to access global configuration view or use command of **interface fastethernet** *interface-number* to access interface configuration view; 2. Use command of **show ipv6 route** to display IPv6 interface information; 3. Done.
Check summary routing information	1. Use command of **disable** to quit back to regular user view or use command of **configure** to access global configuration view, or no command executed to remain in current privilege user view; 2. Use command of **show ip route summary** to display summary routing information; 3. Done.

Appended List:

Parameter	Description	Value
ip-address	Destination IP address	Dotted decimal form, e.g., (A.B.C.D, where A~D is decimal number from 0~255).

Chapter5
QoS Configuration

5.1 Summary

This chapter introduces configurations of QSW-2870 Switch QoS, including its background and basic configuration process.

This chapter includes the following section.

5.2 Queue Scheduling and Congestion Control Configuration

5.2.1 Queue Scheduling and Congestion Control Introduction

Congestion Influence

Congestion is a phenomenon that shortage supply of resources causes forwarding rate decreased and introduction of additional delay.

The bottleneck of link bandwidth will cause congestion. The shortage of resource which is used to deal with data transmitting will cause congestion such as shortage of allocated processor time, buffer and memory. Under current complex network environment with variety of services application, congestion is very common.

Congestion may cause a series of negative effect.

- Congestion increases delay and jitter of message transmission. Excessive delay will cause packet retransmission.
- Congestion decreases effective throughput of network. It results in utilization rate of network resource decreasing.
- Serious congestion will consume a large amount of network resource (especially the storage resources). Unreasonable resource allocation may even lead to system collapse because of resource deadlock.

Queue Technique

The central content of congestion management is as the following.

How to make a scheduling strategy of resource when congestion occurs determines processing order of message forwarding. For congestion management, queue technic is usually used. Use queue algorithm to classify flow and then use one priority algorithm to send flow out. Each queue algorithm is used for specific network flow problem. And it influences allocation of bandwidth resource, delay and jitter importantly.

Queue Scheduling Algorithm Supported of QSW-2870

- SP Priority Queue

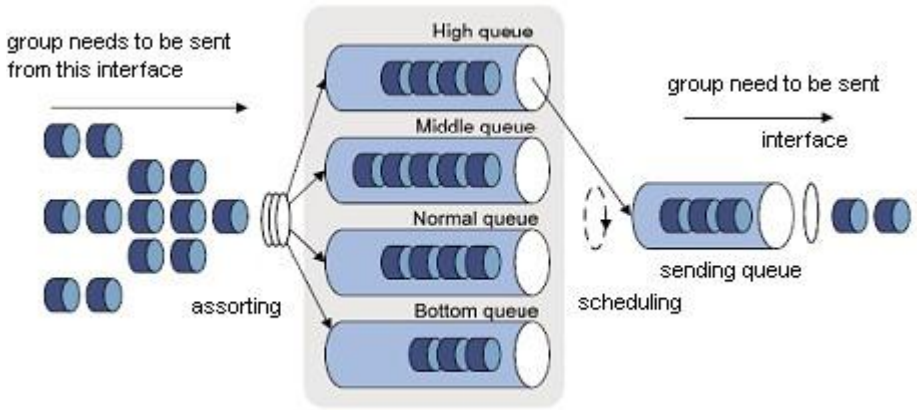


Figure 5-1 SP Queue Scheduling

When using SP (Strict Priority), the packet of higher priority queue is first sent out in strict accordance with priority from high to low order. When higher queue is empty, then send packet of lower priority queue.

Put key service into higher priority queue and non-key service into lower priority queue to guarantee that packet of key service can be sent out first and packet of non-key service can be sent out in the free space of data processing of key service. Usually, Switch chip supports the maximum number of eight queues.

- RR Scheduling Queue

When using RR (Round Robin) and congestion occurs, the output bandwidth of each non-empty output queue is the same and the total equals to the interface bandwidth.

- WRR Weighted Average Queue

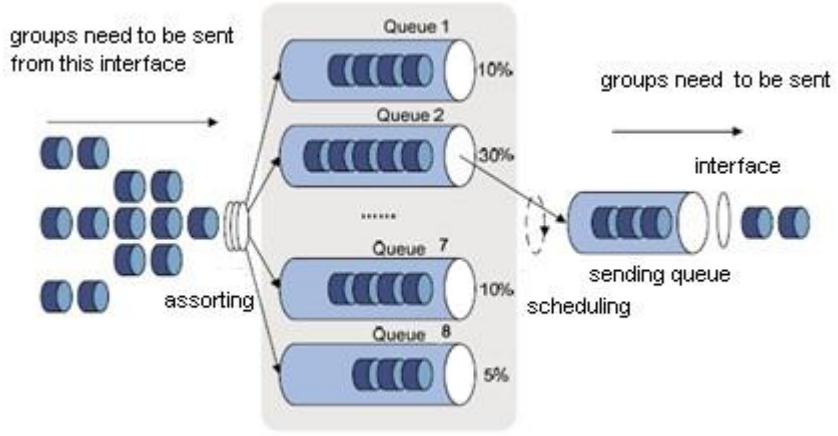


Figure 5-2 WRR Queue Scheduling

WRR (Weighted Round Robin) algorithm is scheduled among ports in turns to guarantee that every queue obtains some service time. When congestion occurring, each non-empty output queue sends out flow according to the bandwidth proportion and its total equals to the available bandwidth of interface.

Advantage1: It guarantees that the lowest priority queue obtains part of bandwidth at least and avoids the problem that message of low priority queue may be not transmitted for a long time when using SP scheduling.

Advantage2: Although multiple queue scheduling is round robin conducted, each queue is not allocated fixed service time slice. If some queue is empty, then change to the next scheduling queue immediately. In this way, bandwidth resource can be fully utilized.

- DRR Scheduling Queue

The scheduling principle of DRR (Deficit Round Robin) is basically the same as WRR scheduling.

The difference between DRR and WRR is as the following.

WRR is a scheduling in accordance with the message number. DRR is a scheduling in accordance with message length. If message length exceeds the capability of queue scheduling, DRR scheduling allows negative weight to guarantee that the long message can be scheduled. But at the next time of round robin, this queue will not be scheduled until its weight is positive.

5.2.2 Configure Queue Scheduling and Congestion Control

Prerequisite

Before configuring queue scheduling and congestion control, it needs to configure filter rule of ACL, please refer to command of 7.2 to configure ACL action to specify interface queue priority for data to pass.

Purpose

Using the operation in this section, when there is congestion in the network, QSW-2870 will deal with message according to the configured scheduling policy so as to balance delay and delay jitter of all kinds of packets. In this way, message of key service can be processed with high priority and non-key service with same priority can be dealt fairly.

Process

According to different destination, please execute corresponding steps. Refer to the following table.

Objective	Procedure
(Optional) Configure scheduling priority of interface queue	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* to enter Interface Configuration View; 3. Use command of **cos queue** *queue-number* **priority** { *priority* | **default** } or use command of **cos queue** *queue-list* **priority** { *priority* | **default** } to configure scheduling priority of interface queue; 4. End.
(Optional) Configure the maximum queue number of interface	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **cos max-queue** { **1** | **8** } to configure the maximum queue number of interface; 3. End.
Configure scheduling mode of	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* to enter

Objective	Procedure
interface queue	Interface Configuration View; 3. Use command of **cos scheduling** { **sp** | **rr** | **wrr** | **drr** } or use command of **cos scheduling** { **sp+rr** | **sp+wrr** | **sp+drr** } *queue-list* to configure scheduling mode of interface queue; 4. End.
(Optional) Configure queue weight of interface	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* to enter Interface Configuration View; 3. Use command of **cos queue** *queue-number* **weight** *weight* or use command of **cos queue** *queue-list* **weight** *weight* to configure queue weight of interface; 4. End.
(Optional) Configure effective bandwidth of queue	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* to enter Interface Configuration View; 3. Use command of **cos queue** { *queue-number* | *queue-list* } { **min-bandwidth** | **max-bandwidth** } **64kbps** *bandwidth-value1* or use command of **cos queue** { *queue-number* | *queue-list* }{ **min-bandwidth** | **max-bandwidth** } **mbps** *bandwidth-value2* to configure effective bandwidth of queue; 4. End.

Attached List:

Parameter	Description	Value
1	queue number to be 1	-
8	queue number to be 8	-
queue-number	queue number	to be from 0 to 7
priority	priority item	to be from 0 to 7
default	default value	1
queue-list	queue list	form as 1,2, to be from 0 to 7
weight	weight item	to be from 0 to100
sp	Strict Priority	-
rr	Round Robin	-
wrr	Weighted Round Robin	-
drr	Deficit Round Robin	-
bandwidth-value1	specify 64Kbps granularity bandwidth	to be from 1 to 16000
bandwidth-value2	specify 1Mbps granularity bandwidth	to be from 1 to1000

5.2.3 Maintenance and Debug

Purpose

When queue scheduling and congestion of QoS function is abnormal, user can use this operation to check or debug.

Process

According to different destination, please execute corresponding steps. Refer to the following table.

Objective	Procedure
Check QoS configuration information of interface	1. Use command of **disable** to exit to Normal User View, or use command of **configure** to enter Global Configuration View, or use command of **interface tunnel** *tunnel-num* to enter Tunnel Interface Configuration View, or no use any command to keep the current Privileged User View; 2. Use command of **show cos interface** or use command of **show cos interface** fastethernet *interface-number* to display QoS configuration information of interface; 3. End.

Attached List:

Parameter	Description	Value
interface-number	interface number	to be <1-12>/<1-18>

5.2.4 Example

5.2.4.1 Configure SP Scheduling

Network Requirements

Flow is from interface 1/0/1, 1/0/2, 1/0/3 of Host1 to Host2. There is congestion on interface 1/0/1 of Host2. Require to use SP algorithm.

Network Diagram

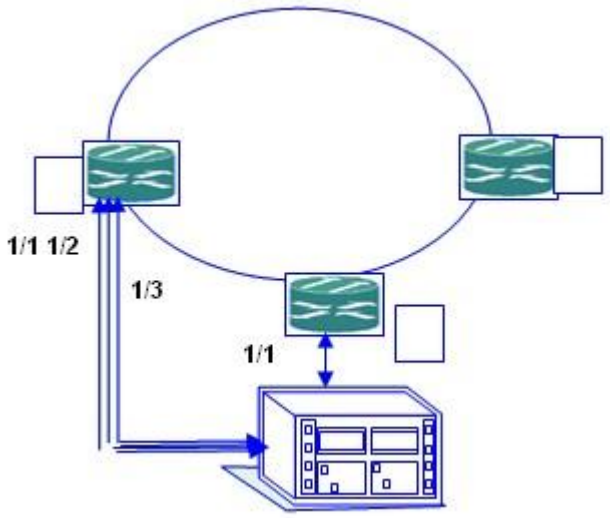


Figure Interface SP Algorithm Topology

Configuration Steps

1. Configure Host1.

//Configure fastethernet **1/0/1.**

S1#configure

S1(config)#interface fastethernet 1/0/1

S1(config-ge1/0/1)#priority 1

S1(config-ge1/0/1)#quit

//Configure fastethernet **1/0/2.**

S1#configure

S1(config)#interface fastethernet 1/0/2

S1(config-ge1/0/2)#priority 2

S1(config-ge1/0/2)#quit

//Configure fastethernet **1/0/3.**

S1#configure

S1(config)#interface fastethernet 1/0/3

S1(config-ge1/0/3)#priority 3

S1(config-ge1/0/3#quit

2. Configure Host2.

//Configure ACL rule.

S2#configure

S2(config)#filter-list 1001

S2(configure-filter-ipv4-1001)#filter 1 ip 10.164.1.0/24 10.164.9.9/32

S2(config-filter1)#filter 1 action cos 7

//Configure fastethernet **1/0/1.**

S2#configure

S2(config)#interface ge 1/0/1

S2(config-ge1/0/1)#cos schedule sp

S2(config-ge1/0/1)#filter-list in 1

Chapter6
IGMP Configuration

6.1 Summary

This chapter introduces configuration of QSW-2870 Switch

IGMP. This chapter includes the following section.

6.2 IGMP Snooping Configuration

6.2.1 IGMP Snooping Introduction

IGMP Snooping Basic Theory

IGMP Snooping is the abbreviation of Internet Group Management Protocol Snooping. It is the multicast restriction mechanism running in the device of Layer-2. This protocol establishes the mapping relationship for port and MAC multicast address by detecting the IGMP message from user host to router in the network and analyzing the received IGMP message. It forwards the multicast data according to this mapping relationship so as to manage and control multicast group.

When the IGMP Snooping does not run in the Layer-2 device, the multicast data is broadcast in the Layer-2. When the IGMP Snooping runs in the Layer-2 device, the known multicast data will not be broadcast in the Layer-2 but will be multicast to the designated receiver.

IGMP Snooping Advantages

IGMP Snooping has the following advantages.

- Enhance the security of multicast information;
- Reduce the broadcast message of Layer-2 network and save the bandwidth;
- Provide convenience for separate account for each user host.

Supporting IGMP Snooping Characteristic of QSW-2870

- Support Static Layer 2 Multicast

  When the multicast message is transmitting in the Ethernet, the destination of message is not a specified receiver but is a group with uncertain member. So when the multicast message is forwarded to de link layer from the network layer, it cannot generate multicast forwarding table which leads to using broadcast way to transmit multicast message in the link layer. When the device is deployed between router and user host and applies Layer-2 forwarding characteristic, it can transmit multicast data to the user who needs to receive the data for long time by configuring static Layer-2 multicast (manually configure forwarding table).

  Static Layer-2 multicast has the following characteristics.

  Configure interface to join multicast group statically to avoid protocol message attack.

  Use the mechanism of directly searching multicast message forwarding table for forwarding message to reduce network delay.

  Avoid unregistered user receiving multicast message and provide paid service.

- Support Multicast VLAN Copy

  In traditional multicast forwarding mode, when users belonging to different VLAN demand for the same multicast source, Switch needs to copy one multicast data for each VLAN and then transmit to every VLAN. After configuring multicast VLAN copy, when users belonging to different VLAN demand for the same multicast source, Switch will configure one multicast VLAN for all these VLANs. In this way, the upper router only needs transmit one set of data to this multicast VLAN but does not need to copy a set of multicast data for each VLAN.

  It can facilitate managing and controlling the multicast source and multicast group member and also can reduce the waste of bandwidth and network extra burden.

- Support IGMP Snooping Based on VLAN

  IGMP version can be configured to be V1/V2/V3.

  Multicast Forwarding Mode can be configured.

  Support static routing interface.

Support IGMP query function.

Support IGMP message suppression.

Support interface fast leave.

Aging time of routing interface can be configured.

The maximum response interval of group member can be configured.

Multicast policy can be configured.

Router Alert option can be configured.

The source IP address of sending IGMP message can be configured.

Support IGMP Proxy function.

- Support Controllable Multicast

  Controllable multicast is a part of the IPTV multicast scheme. It is mainly applied in the multicast environment of Layer-2 to control program number of IPTV and to ensure the quality of service for the majority of users.

  This characteristic has the following advantage.

  Precise control of multicast service

  Ensure the quality of service for the majority of users.

  Reduce the harm of multicast attack to a certain extent.

6.2.2 Configure Static Layer 2 Multicast

Background

In Metro Ethernet, when user host needs to receive multicast data flow of some multicast group, interface can be configured to join in the multicast group.

Purpose

After configuring this function, user can receive registered multicast data flow stably and timely for long time.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step
Globally enable IGMP Snooping	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **igmp-snooping start** to globally enable IGMP Snooping; 3. Done.
Create multicast VLAN	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **vlan** *vlan-list* to create VLAN which should be enabled IGMP Snooping; 3. Use command of **igmp-snooping mvlan** *vlan-id* to create corresponding multicast VLAN and enter the multicast VLAN configuration view; 4. Done.
(Optional) Configure multicast data forwarding mode of multicast VLAN	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **igmp-snooping mvlan** *vlan-id* to enter the multicast VLAN configuration view; 3. Use command of **igmp-snooping forwarding-mode** { **ip | mac** } to configure multicast data forwarding mode; 4. Done.
Configure interface to join in VLAN and enable IGMP Snooping on interface	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* to enter the Interface Configuration View; 3. Use command of **port hybrid vlan** *vlan-list* { **tagged** | **untagged** } to configure interface to join in VLAN; 4. Use command of **igmp-snooping enable** to enable IGMP Snooping function on interface; 5. Done.
Configure interface to join in static multicast group	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* to enter the Interface Configuration View; 3. Use command of **igmp-snooping static-group group-address** *group-address* **mvlan** *vlan-id* to configure interface to join in static multicast group; 4. Done.

Appendix List:

Parameter	Description	Value
vlan-id	VLAN ID	integer with range of 1-4094
interface-number	Ethernet port number	integer with range of <1-8>/<0-4>/<1-48>
group-address	multicast IP address	224.0.0.0 -239.255.255.255

Parameter	Description	Value
ip	forward multicast data according to IP address	-
mac	forward multicast data according to MAC address	-

6.2.3 Configure Multicast VLAN Copy

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step
Globally enable IGMP Snooping	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **igmp-snooping start** to globally enable IGMP Snooping; 3. Done.
Create multicast VLAN	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **vlan** *vlan-list* to create VLAN which should be enabled IGMP Snooping; 3. Use command of **igmp-snooping mvlan** *vlan-id* to create corresponding multicast VLAN and enter the multicast VLAN configuration view; 4. Done.
Configure multicast data forwarding mode of multicast VLAN to be IP	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **igmp-snooping mvlan** *vlan-id* to enter the multicast VLAN configuration view; 3. Use command of **igmp-snooping forwarding-mode ip** to configure multicast data forwarding mode to be IP; 4. Done.
Enable multicast copy function of multicast VLAN	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **igmp-snooping mvlan** *vlan-id* to enter the multicast VLAN configuration view; 3. Use command of **igmp-snooping multicast-vlan enable** to enable multicast VLAN copy function; 4. Done.
Configure user VLAN	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **igmp-snooping mvlan** *vlan-id* to enter the multicast VLAN configuration view; 3. Use command of **igmp-snooping multicast user-vlan** *vlan-list* to configure user VLAN; 4. Done.
Configure	1. Use command of **configure** to enter the Global Configuration View;

Objective	Step
interface to join in VLAN and enable IGMP Snooping protocol on interface	2. Use command of **interface fastethernet** *interface-number* to enter the Interface Configuration View; 3. Use command of **port hybrid vlan** *vlan-list* { **tagged** | **untagged** } to configure interface to join in VLAN; 4. Use command of **igmp-snooping enable** to enable IGMP Snooping function on interface; 5. Done.

Appendix List:

Parameter	Description	Value
vlan-id	VLAN item	integer with range of 1-4094
vlan-list	VLAN list	integer with range of 1~4094, form as 1,3-5

6.2.4 Configure IGMP Snooping

Background

IGMP Snooping based on VLAN runs on the Switch between router and user host. By listening the IGMP Snooping message sent between upper router and host to maintain the IGMP message forwarding table, so it can manage and control to transmit the multicast data message to realize the multicast of Layer-2.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step
Globally enable IGMP Snooping	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **igmp-snooping start** to globally enable IGMP Snooping; 3. Done.
Create multicast VLAN	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **vlan** *vlan-list* to create VLAN which should be enabled IGMP Snooping; 3. Use command of **igmp-snooping mvlan** *vlan-id* to create corresponding multicast VLAN and enter the multicast VLAN configuration view; 4. Done.
Configure multicast data	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **igmp-snooping mvlan** *vlan-id* to enter the multicast

Objective	Step
forwarding mode of multicast VLAN	VLAN configuration view; 3. Use command of **igmp-snooping forwarding-mode** { **ip | mac** } to configure multicast data forwarding mode; 4. Done.
(Optional) Configure IGMP version	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **igmp-snooping mvlan** *vlan-id* to enter the multicast VLAN configuration view; 3. Use command of **igmp-snooping version** { **v1** | **v2** | **v3** } to confiugre IGMP version; 4. Done.
(Optional) Configure static router interface	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **igmp-snooping mvlan** *vlan-id* to enter the multicast VLAN configuration view; 3. Use command of **igmp-snooping uplink-port fastethernet** *interface-number* to configure static router interface 4. Done.
(Optional) Configure query parameter	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **igmp-snooping query-interval** *query-interval* to configure the interval of sending query message (all multicast VLAN share to use this parameter); 3. Use command of **igmp-snooping robust-count** *robust-count* to configure IGMP robust coefficient of query (all multicast VLAN share to use this parameter); 4. Use command of **igmp-snooping lastmember-queryinterval** *query-Interval* to configure query interval of specific group query (all multicast VLAN share to use this parameter); 5. Use command of **igmp-snooping lastmember-querynumber** *query-number* to configure specific query time (all multicast VLAN share to use this parameter); 6. Use command of **igmp-snooping mvlan** *vlan-id* to enter the multicast VLAN configuration view; 7. Use command of **igmp-snooping querier** { **enable** | **disable** } to configure IGMP Snooping query enabled state; 8. Use command of **igmp-snooping max-response-time** *response-time* to configure the maximum response time fileld value of general query message; 9. Done.
(Optional) Configure multicast policy	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **igmp-snooping mvlan** *vlan-id* to enter the multicast VLAN configuration view;

Objective	Step
	3. Use command of **igmp-snooping group-policy filter-list** *filter-number* **version** *version-List* to configure multicast policy; 4. Done.
(Optional) Configure protocol message suppression	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **igmp-snooping mvlan** *vlan-id* to enter the multicast VLAN configuration view; 3. Use command of **igmp-snooping report-suppress** { **enable** | **disable** } to configure the enabled state of message suppression in VLAN; 4. Done.
(Optional) Configure the source IP of query message	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **igmp-snooping mvlan** *vlan-id* to enter the multicast VLAN configuration view; 3. Use command of **igmp-snooping proxy-ip** *ip-address* to configure the source IP of query message, this configuration is effective only enabling message suppression or working in proxy; 4. Done.
(Optional) Configure router-alert option	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **igmp-snooping mvlan** *vlan-id* to enter the multicast VLAN configuration view; 3. Use command of **igmp-snooping require-router-alert** { **enable** | **disable** } to configure router-alert requirement, only deal with the IGMP message with router-alert option after enabling this function; 4. Done.
(Optional) Configure multicast VLAN working mode	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **igmp-snooping mvlan** *vlan-id* to enter the multicast VLAN configuration view; 3. Use command of **igmp-snooping workmode** { **igmp-proxy** | **igmp-snooping** } to configure multicast VLAN working mode to be snooping or proxy; 4. Done.
(Optional) Configure interface to leave fast	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* to enter the Interface Configuration View; 3. Use command of **igmp-snooping fast-leave** { **enable** | **disable** } to configure interface to leave fast; 4. Done.

Appendix List:

Parameter	Description	Value
vlan-id	VLAN ID	integer, to be1-4094

Parameter	Description	Value
interface-number	Ethernet interface port number	integer with range of <1-8>/<0-4>/<1-48>
query-interval	time range of query interval	integer, to be10-65535
robust-count	the time of sending specific query message, indicate the IGMP robust coefficient of current VLAN	integer with range of 2-5
query-number	specific query time range	integer with range of 2-16
query-interval	specific query interval range	integer with range of 1-5, unit: second
max-response-time	the maximum response time range	integer with range of 1-25, unit: second
ip-address	destination IP address	dotted decimal, form as A.B.C.D, A~D is 0~255

6.2.5 Configure Controllable Multicast

Purpose

It is usually used in the multicast of Layer-2 scenarios to control IPTV program number and guarantee the service quality of most users.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step
Configure IGMP Snooping function based on VLAN	The realization of controllable multicast base on IGMP Snooping function, the configuration step of IGMP Snooping refers to 6.2.4;
Configure controllable channel parameter	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **igmp-control channel** *NAME* **mvlan** *vlan-Id* **group-address** *groupIp* **source-address** *srcIp* to create and configure channel parameter (source-address is now non-effective provisionally); 3. Done.
(Optional) Configure the maximum user number of controllable channel	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **igmp-control channel** *NAME* **max-user-number** *max-number* to configure the maximum user number of controllable channel; 3. Done.
Configure	1. Use command of **configure** to enter the Global Configuration View;

Objective	Step
controllable preview template	2. Use command of **igmp-control preview-profile** *NAME* **time-total** *time* to configure preview template of total time mode; 3. Use command of **igmp-control preview-profile** *NAME* **time-sharing count** *count* **duration** *duration-time* **interval** *interval-time* to configure preview template of sharing time mode; 4. Done.
Configure controllable program package	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **igmp-control package** *NAME* **channel** *channel-name* { **deny** | **watch** } to add channel into the program package with forbiddance or viewing permission authority; 3. Use command of **igmp-control package** *NAME* **channel** *channel-name* **preview** *preview-profile-name* to add channel into the program package with preview mode; 4. Done.
Configure controllable multicast user	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* to enter the Interface Configuration View; 3. Use command of **igmp-snooping ctrlmode** { **enable** | **disable** } to enable controllable function of interface; 4. Use command of **igmp-control auth package** *packet-name* to create controllable user based on interface and authenticate the binding program package; 5. Use command of **igmp-control no-auth** to create super user based on interface who can view all channels; 6. Use command of **igmp-control vlan** *vlan-Id* **auth package** *package-name* to create controllable user based on interface and VLAN and authenticate the binding program package; 7. Use command of **igmp-control vlan** *vlan-Id* **no-auth** to create super user based on interface and VLAN who can view all channels in VLAN; 8. Done.
(Optional) Configure the maximum channel number of controllable multicast user	1. Use command of **configure** to enter the Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* to enter the Interface Configuration View; 3. Use command of **igmp-control max-channel** *channel-number* to configure the maximum viewing channel number of user based on interface; 4. Use command of **igmp-control vlan** *vlan-Id* **max-channel** *channel-number* to configure the maximum viewing channel number of controllable multicast user;

Objective	Step
	5. Done.

6.2.6 Maintenance and Debug

Purpose

When IGMP Snooping is abnormal and it needs to check, debug or locate problem, user can use operation of this section.

Procedure

According to the different purposes, execute corresponding step. Please refer to the following table.

Objective	Step
Enable IGMP Snooping debug function	1. Use command of **disable** to exit to the Common User View or Keep current Privilege User View; 2. Use command of **debug igmpsnoop** to enable IGMP Snooping debug function; 3. Done.
Disable IGMP Snooping debug function	1. Use command of **disable** to exit to the Common User View or Keep current Privilege User View; 2. Use command of **no debug igmpsnoop** to disable IGMP Snooping debug function; 3. Done.
Check IGMP Snooping configuration file information	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface fastethernet** *interface-number* to enter the Interface Configuration View; 2. Use command of **show igmp-snooping config** to check IGMP Snooping configuration file information; 4. Done.
Check IGMP Snooping interface configuration file information	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface fastethernet** *interface-number* to enter the Interface Configuration View; 2. Use command of **show igmp-snooping interface** to display IGMP Snooping interface configuration file information ; 3. Done.
Check IGMP Snooping	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use

Objective	Step
multicast VLAN configuration file information	command of **interface fastethernet** *interface-number* to enter the Interface Configuration View; 2. Use command of **show igmp-snooping mvlan** to display IGMP Snooping multicast VLAN configuration file information; 3. Done.
Check IGMP Snooping router interface configuration file information	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface fastethernet** *interface-number* to enter the Interface Configuration View; 2. Use command of **show igmp-snooping uplinkport** to display IGMP Snooping router interface configuration file information ; 3. Done.
Check IGMP Snooping table information of all or designated interface or designated VLAN egress interface	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface fastethernet** *interface-number* to enter the Interface Configuration View; 2. Use command of show igmp-snooping egress-port or show igmp-snooping egress-port mvlan *vlan-id* or show igmp-snooping egress-port interface **fastethernet** *interface-number* to display IGMP Snooping egress interface table information; 3. Done.
Check IGMP Snooping multicast group table information	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface fastethernet** *interface-number* to enter the Interface Configuration View; 2. Use command of **show igmp-snooping group** to display IGMP Snooping multicast group table information; 3. Done.
Check IGMP Snooping multicast source table information(only effective of version3)	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface fastethernet** *interface-number* to enter the Interface Configuration View; 2. Use command of **show igmp-snooping source-address** to display IGMP Snooping multicast source table information; 3. Done.
Check IGMP Snooping SSM Map configuration file information	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface fastethernet** *interface-number* to enter the Interface Configuration View; 2. Use command of **show igmp-snooping ssm-mapping** to diplay IGMP

Objective	Step
	Snooping SSM Map configuration file information; 3. Done.
Check channel configuration of controllable multicast	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface fastethernet** *interface-number* to enter the Interface Configuration View; 2. Use command of **show igmp-control channel** to display channel configuration of controllable multicast; 3. Done.
Check preview template configuration of controllable multicast	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface fastethernet** *interface-number* to enter the Interface Configuration View; 2. Use command of **show igmp-control preview-profile** { *NAME* } to display preview template configuration of controllable multicast; 3. Done.
Check program package configuration information of controllable multicast	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface fastethernet** *interface-number* to enter the Interface Configuration View; 2. Use command of **show igmp-control package** { *NAME* } to display program package configuration information of controllable multicast; 3. Done.
Check user configuration information of controllable multicast	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface fastethernet** *interface-number* to enter the Interface Configuration View; 2. Use command of **show igmp-control interface user** to display controllable user configuration file information based on interface; 3. Use command of **show igmp-control interface-vlan user** to display controllable user configuration file information based on interface and VLAN; 4. Done.
Check online user information of controllable multicast	1. Use command of **disable** to exit to the Common User View or use command of **configure** to enter the Global Configuration View or use command of **interface fastethernet** *interface-number* to enter the Interface Configuration View; 2. Use command of **show igmp-control interface online-user** to display online user information based on interface; 3. Use command of **show igmp-control interface-vlan online-user** to display online user information based on interface and VLAN;

Objective	Step
	4. Done.

Appendix List:

Parameter	Description	Value
interface-number	Ethernet interface number	integer with range of <1-8>/<0-4>/<1-48>
vlan-id	VLAN ID	integer with range of 1-4094
NAME	-	character string

6.2.7 Example

6.2.7.1 Example for Static Layer 2 Multicast

Network Requirement

Switch interface GE1/0/1 connects with the router of the multicast source side. Interface GE1/0/2 connects with user host. It requires that all hosts in VLAN100 can receive the multicast data of the IP 225.1.1.1 for long time.

Network Topology

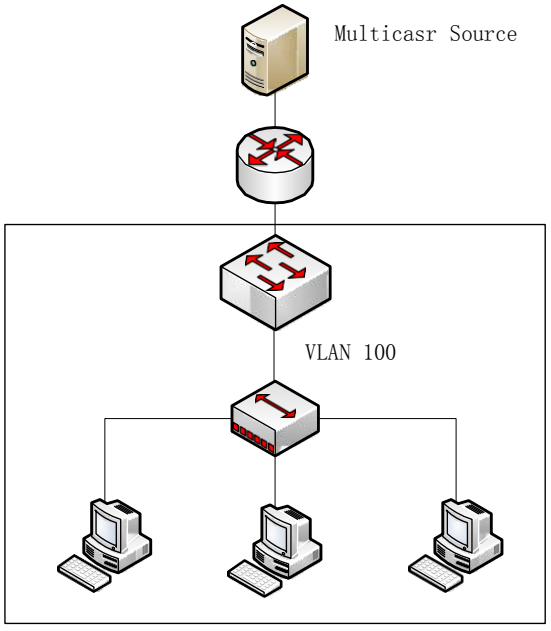


Figure Static Layer 2 Multicast Topology

Configuration Step

1. Globally enable IGMP Snooping function.

Switch#configure

Switch(config)#igmp-snooping start

Switch(config)#

2. Create VLAN and corresponding multicast VLAN and configure interface to join in the VLAN.

Switch(config)#vlan 100

Switch(vlan-100)#quit

Switch(config)#interface fastethernet 1/0/1

Switch(config-ge1/0/1)#port hybrid vlan 100 tagged

Switch(config-ge1/0/1)#quit

Switch(config)#interface fastethernet 1/0/2

Switch(config-ge1/0/2)#port hybrid vlan 100 tagged

Switch(config-ge1/0/2)#quit

Switch(config)# igmp-snooping mvlan 100

Switch(config-igmpsnoop-mvlan100)#quit

Switch(config)#

3. Enable IGMP Snooping on interface.

Switch(config)#interface fastethernet 1/0/1

Switch(config-ge1/0/1)#igmp-snooping enable

Switch(config-ge1/0/1)#quit

Switch(config)#interface fastethernet 1/0/2

Switch(config-ge1/0/2)#igmp-snooping enable

Switch(config-ge1/0/2)#quit

Switch(config)#

4. Configure interface GE1/0/1 to be the static router interface.

Switch(config)#igmp-snooping mvlan 100

Switch(config-igmpsnoop-mvlan100)#igmp-snooping uplink-port fastethernet 1/0/1

Switch(config-igmpsnoop-mvlan100)#quit

Switch(config)#

5. Configure static multicast group.

Switch(config)#interface fastethernet 1/0/2

Switch(config-ge1/0/2)#igmp-snooping static-group group-address 225.1.1.1 mvlan 100

Switch(config-ge1/0/2)#quit

```
Switch(config)#
```

6. Check multicast group table and egress interface table information.

```
Switch#show igmp-snooping group
  Total Entry(s) : 1
  Group Address     MVlan    Pre-join    MemNum    V3FilterMode
  225.1.1.1           100       disable     1           invalid

Switch#show igmp-snooping egress-port
Total Entry(s) : 1

Group Address : 225.1.1.1
MVlan : 100
Source Address : *
Interface : ge-1/0/2
    Type : static
    Expires : ---
   OutVlan :      100
    V3 Mode : invalid
```

6.2.7.2 Example for IGMP Snooping

Network Requirement

Switch interface GE1/0/1 connects with the router of the multicast source side. Interface GE1/0/2 connects with user host. It requires that the three host can receive the multicast data with IP address of 225.1.1.1~225.1.1.2 in VLAN100 for long time by configuring IGMP Snooping function.

Network Topology

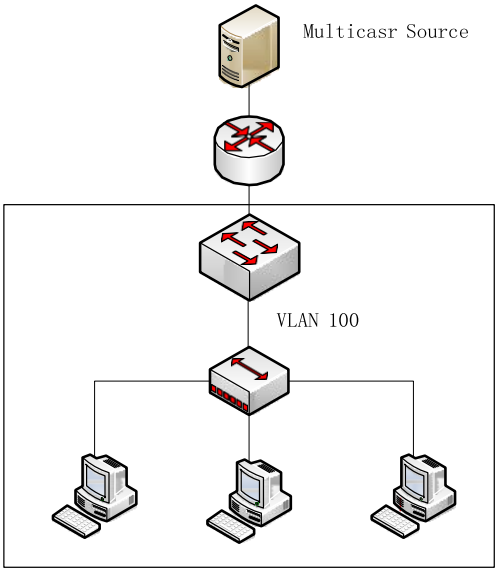


Figure IGMP Snooping Configuration Topology

Configuration Step

1. Globally enable IGMP Snooping function.

Switch#configure

Switch(config)#igmp-snooping start

Switch(config)#

2. Create VLAN and corresponding multicast VLAN and configure interface to join in the VLAN.

Switch(config)#vlan 100

Switch(vlan-100)#quit

Switch(config)#interface fastethernet 1/0/1

Switch(config-ge1/0/1)#port hybrid vlan 100 tagged

Switch(config-ge1/0/1)#quit

Switch(config)#interface fastethernet 1/0/2

Switch(config-ge1/0/2)#port hybrid vlan 100 tagged

Switch(config-ge1/0/2)#quit

Switch(config)# igmp-snooping mvlan 100

Switch(config-igmpsnoop-mvlan100)#quit

Switch(config)#

3. Enable IGMP Snooping function on interface.

Switch(config)#interface fastethernet 1/0/1

Switch(config-ge1/0/1)#igmp-snooping enable

Switch(config-ge1/0/1)#quit

Switch(config)#interface fastethernet 1/0/2

Switch(config-ge1/0/2)#igmp-snooping enable

Switch(config-ge1/0/2)#quit

Switch(config)#

4. Confiugre interface GE1/0/1 to be static router interface.

Switch(config)#igmp-snooping mvlan 100

Switch(config-igmpsnoop-mvlan100)#igmp-snooping uplink-port fastethernet 1/0/1

Switch(config-igmpsnoop-mvlan100)#quit

Switch(config)#

5. Configure static multicast group.

Switch(config)#interface fastethernet 1/0/2

Switch(config-ge1/0/2)#igmp-snooping static-group group-address 225.1.1.1 mvlan 100

Switch(config-ge1/0/2)#igmp-snooping static-group group-address 225.1.1.2 mvlan 100

Switch(config-ge1/0/2)#quit

Switch(config)#

6. Check multicast group table and egress interface table information.

Switch#show igmp-snooping group

Total Entry(s) : 2

Group Address	MVlan	Pre-join	MemNum	V3FilterMode
225.1.1.1	100	disable	1	invalid
225.1.1.2	100	disable	1	invalid

Switch#show igmp-snooping egress-port

Total Entry(s) : 2

Group Address : 225.1.1.1

MVlan : 100

Source Address : *

Interface : ge-1/0/2

Type : static

Expires : ---

OutVlan : 100
V3 Mode : invalid
Group Address : 225.1.1.2
MVlan : 100
Source Address : *
Interface : ge-1/0/2
Type : static
Expires : ---
OutVlan : 100
V3 Mode : invalid

6.2.7.3 Example for Multicast VLAN Copy

Network Requirement

Switch interface GE1/0/1 connects with the router of the multicast source side belonging to VLAN100. Interface GE1/0/2 and GE1/0/3 connects with user host and separately belongs to VLAN2 and VLAN3. It requires that the four hosts connecting with the Switch can receive the multicast data with IP address of 225.0.0.1~225.0.0.3. VLAN100 is the multicast VLAN. VLAN3 and VLAN4 are user VLANs.

Network Topology

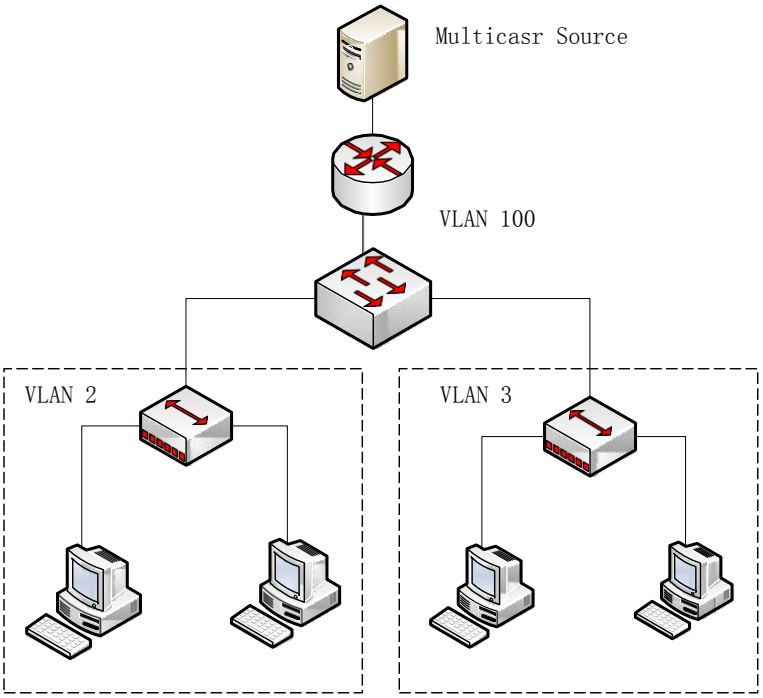


Figure Multicast Copy Topology

Configuration Step

1. Globally enable IGMP Snooping function.

Switch#configure

Switch(config)# igmp-snooping start

Switch(config)#

2. Create VLAN and corresponding multicast VLAN and configure interface to join in the VLAN.

Switch(config)#vlan 2,3,100

Switch(config)#interface fastethernet 1/0/1

Switch(config-ge1/0/1)#port hybrid vlan 100 tagged

Switch(config-ge1/0/1)#quit

Switch(config)#interface fastethernet 1/0/2

Switch(config-ge1/0/2)#port hybrid vlan 2 tagged

Switch(config-ge1/0/2)#quit

Switch(config)#interface fastethernet 1/0/3

Switch(config-ge1/0/3)#port hybrid vlan 3 tagged

Switch(config-ge1/0/3)#quit

Switch(config)# igmp-snooping mvlan 100

Switch(config-igmpsnoop-mvlan100)#quit

Switch(config)#

3. Enable IGMP Snooping function on interface.

Switch(config)#interface fastethernet 1/0/1

Switch(config-ge1/0/1)#igmp-snooping enable

Switch(config-ge1/0/1)#quit

Switch(config)#interface fastethernet 1/0/2

Switch(config-ge1/0/2)#igmp-snooping enable

Switch(config-ge1/0/2)#quit

Switch(config)#interface fastethernet 1/0/3

Switch(config-ge1/0/3)#igmp-snooping enable

Switch(config-ge1/0/3)#quit

Switch(config)#

4. Enable multicast copy function in multicast VLAN and configure user VLAN.

Switch(config)#igmp-snooping mvlan 100

Switch(config-igmpsnoop-mvlan100)#igmp-snooping forwarding-mode ip

Switch(config-igmpsnoop-mvlan100)#igmp-snooping multicast-vlan enable

Switch(config-igmpsnoop-mvlan100)#igmp-snooping multicast user-vlan 2,3

Switch(config-igmpsnoop-mvlan100)#quit

Switch(config)#

5. Confiugre interface GE1/0/1 to be static router interface.

Switch(config)#igmp-snooping mvlan 100

Switch(config-igmpsnoop-mvlan100)#igmp-snooping uplink-port fastethernet 1/0/1

Switch(config-igmpsnoop-mvlan100)#quit

Switch(config)#

6. Confiugre static multicast group.

Switch(config)#interface fastethernet 1/0/2

Switch(config-ge1/0/2)#igmp-snooping static-group group-address 225.0.0.1 mvlan 100 user-vlan 2

Switch(config-ge1/0/2)#igmp-snooping static-group group-address 225.0.0.2 mvlan 100 user-vlan 2

Switch(config-ge1/0/2)#igmp-snooping static-group group-address 225.0.0.3 mvlan 100 user-vlan 2

Switch(config-ge1/0/2)#quit

Switch(config)#interface fastethernet 1/0/3

Switch(config-ge1/0/3)#igmp-snooping static-group group-address 225.0.0.1 mvlan 100 user-vlan 3

Switch(config-ge1/0/3)#igmp-snooping static-group group-address 225.0.0.2 mvlan 100 user-vlan 3

Switch(config-ge1/0/3)#igmp-snooping static-group group-address 225.0.0.3 mvlan 100 user-vlan 3

Switch(config-ge1/0/3)#quit

7. Check multicast group table and egress interface table information.

Switch#show igmp-snooping group

Total Entry(s) : 3

Group Address	MVlan	Pre-join	MemNum	V3FilterMode
225.0.0.1	100	disable	2	invalid
225.0.0.2	100	disable	2	invalid
225.0.0.3	100	disable	2	invalid

Switch#show igmp-snooping egress-port

Total Entry(s) : 6

Group Address : 225.0.0.1

MVlan : 100

Source Address : *

Interface : ge-1/0/2

Type : static

Expires : ---

OutVlan : 2

V3 Mode : invalid

Group Address : 225.0.0.1

MVlan : 100

Source Address : *

Interface : ge-1/0/3

Type : static

Expires : ---

OutVlan : 3

V3 Mode : invalid

Group Address : 225.0.0.2

MVlan : 100

Source Address : *
Interface : ge-1/0/2
Type : static
Expires : ---
OutVlan : 2
V3 Mode : invalid
Group Address : 225.0.0.2
MVlan : 100
Source Address : *
Interface : ge-1/0/3
Type : static
Expires : ---
OutVlan : 3
V3 Mode : invalid
Group Address : 225.0.0.3
MVlan : 100
Source Address : *
Interface : ge-1/0/2
Type : static
Expires : ---
OutVlan : 2
V3 Mode : invalid
Group Address : 225.0.0.3
MVlan : 100
Source Address : *
Interface : ge-1/0/3
Type : static
Expires : ---
OutVlan : 3
V3 Mode : invalid

6.2.7.4 Example for Controllable Multicast

Network Requirement

Switch interface GE1/0/1 connects with the router of the multicast source side. Interface GE1/0/2 and GE1/0/3 connects with user host. It requires that the user of

GE1/0/2 can view the 225.1.1.1 channel, preview 225.1.1.2 channel and deny to view 225.1.1.3 channel. It requires that the user of GE1/0/3 can view 225.1.1.2 channel, preview 225.1.1.3 channel and deny viewing 225.1.1.1 channel.

Network Topology

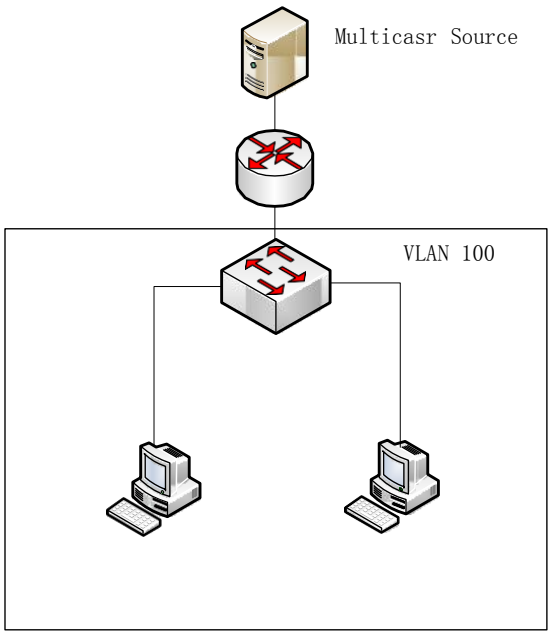


Figure Controllable Multicast Topology

Configuration Step

1. Globally enable IGMP Snooping function.

Switch#configure

Switch(config)# igmp-snooping start;

Switch(config)#

2. Create VLAN and corresponding multicast VLAN and configure interface to join in the VLAN.

Switch(config)#vlan 100

Switch(vlan-100)#quit

Switch(config)#interface fastethernet 1/0/1

Switch(config-ge1/0/1)#port hybrid vlan 100 tagged

Switch(config-ge1/0/1)#quit

Switch(config)#interface fastethernet 1/0/2

Switch(config-ge1/0/2)#port hybrid vlan 100 tagged

Switch(config-ge1/0/2)#quit

Switch(config)#interface fastethernet 1/0/3

Switch(config-ge1/0/3)#port hybrid vlan 100 tagged

Switch(config-ge1/0/3)#quit

Switch(config)# igmp-snooping mvlan 100

Switch(config-igmpsnoop-mvlan100)#quit

Switch(config)#

3. Enable IGMP Snooping function on interface.

Switch(config)#interface fastethernet 1/0/1

Switch(config-ge1/0/1)#igmp-snooping enable

Switch(config-ge1/0/1)#quit

Switch(config)#interface fastethernet 1/0/2

Switch(config-ge1/0/2)#igmp-snooping enable

Switch(config-ge1/0/2)#quit

Switch(config)#interface fastethernet 1/0/3

Switch(config-ge1/0/3)#igmp-snooping enable

Switch(config-ge1/0/3)#quit

Switch(config)#

4. Cretae controllable multicast channel.

Switch(config)#igmp-control channel channel-1 mvlan 100 group-address 225.1.1.1 source-address 0.0.0.0

Switch(config)#igmp-control channel channel-2 mvlan 100 group-address 225.1.1.2 source-address 0.0.0.0

Switch(config)#igmp-control channel channel-3 mvlan 100 group-address 225.1.1.3 source-address 0.0.0.0

5. Create controllable multicast preview template.

Switch(config)#igmp-control preview-profile pp-1 time-total 60

6. Create two program packages.

Switch(config)#igmp-control package pkg-1 channel channel-1 watch

Switch(config)#igmp-control package pkg-1 channel channel-2 preview pp-1

Switch(config)#igmp-control package pkg-1 channel channel-3 deny

Switch(config)#igmp-control package pkg-2 channel channel-2 watch

Switch(config)#igmp-control package pkg-2 channel channel-3 preview pp-1

Switch(config)#igmp-control package pkg-2 channel channel-1 deny

7. Create authority user based on interface of GE1/0/2 and bind with program package of pkg-1.

```
Switch(config)#interface fastethernet 1/0/2
Switch(config-ge1/0/2)#igmp-snooping ctrlmode enable
Switch(config-ge1/0/2)#igmp-control auth package pkg-1
Switch(config-ge1/0/2)#quit
Switch(config)#
```

8. Create authority user based on interface of GE1/0/3 and bind with program package of pkg-2.

```
Switch(config)#interface fastethernet 1/0/3
Switch(config-ge1/0/3)#igmp-snooping ctrlmode enable
Switch(config-ge1/0/3)#igmp-control auth package pkg-2
Switch(config-ge1/0/3)#quit
Switch(config)#
```

9. Check configuration result.

```
Switch#show igmp-control channel
  Total Entry(s) : 3
 Channal Name            Vlan    Group-ip        Source-ip          Max-user
1        channel-1          100   225.1.1.1       0.0.0.0             256
2        channel-2          100   225.1.1.2       0.0.0.0             256
3        channel-3          100   225.1.1.3       0.0.0.0             256

Switch#show igmp-control preview-profile pp-1
 Preview:        1
Type:            time-total
Total time:    60

Switch#show igmp-control package pkg-1
 Channel-Count   3
 Preview-Count   1
 Channel   Name        Vlan          Group-ip          Source-ip      Rights
 1         channel-1   vlan-100      225.1.1.1         0.0.0.0        watch
 2         channel-2   vlan-100      225.1.1.2         0.0.0.0        preview(1)
 3         channel-3   vlan-100      225.1.1.3         0.0.0.0        deny

Switch#show igmp-control package pkg-2
 Channel-Count   3
```

Preview-Count : 1

Channel	Name	Vlan	Group-ip	Source-ip	Rights
1	channel-1	vlan-100	225.1.1.1	0.0.0.0	deny
2	channel-2	vlan-100	225.1.1.2	0.0.0.0	watch
3	channel-3	vlan-100	225.1.1.3	0.0.0.0	preview(1)

Switch#show igmp-control interface user

Interface	Auth	Package	MaxChannel	OnlineChannel
ge-1/0/2	enable	pkg-1	128	0
ge-1/0/3	enable	pkg-2	128	0

Chapter7
Security Configuration

7.1 Summary

This chapter mainly introduces related security configuration of QSW-2870 including 802.1x, AAA, RADIUS, ACL configuration and etc.

This chapter includes the following section.

7.2 ACL Configuration


Note:

In this section, ACL means access control list for IPv4 message, ACL6 means access control list for IPv6 message.

7.2.1 ACL Introduction

ACL Function

User can configure rules and action of ACL (Access Control List) to determine which kind of data is allowed to pass or to deny so as to control data transmission and to improve network performance and guarantee service security.

ACL is a series of sequential rules and action composed of layer2 MAC and layer3 IP. Using the rules to filter data packet according to the source and destination address and port number of data. Applying ACL to QSW-2870, device determines which data to be received or to deny and other action to deal with the data according the rules of ACL.

ACL classification supported of QSW-2870

QSW-2870 supports Layer2 ACL, Layer3 ACL, Mixed ACL and Layer3 ACL6.

- Layer2 ACL: Mainly based on source MAC, destination MAC, VLAN, priority, protocol type, rate limitation template, time-range template and etc. to classify the data.
- Layer3 ACL: Mainly based on source IP, destination IP, source port number, destination port number, protocol type, priority, fragment, lifetime, rate limitation template, time-range template and etc. to classify the data.
- Mixed ACL: Mainly based on source MAC, destination MAC, source IP, destination IP, source port number, destination port number, protocol type, priority, VLAN, rate limitation template, time-range template and etc. to classify the data.
- Layer3 ACL6: Mainly based on source IPv6, destination IPv6, source port number, destination port number, protocol type, hop limitation, the next head, traffic class, flow flag, rate limitation template, time-range template and etc. to classify the data.

7.2.2 Configure Layer2 ACL

Background Information

One ACL is composed of some rules and actions.

Before configuring Layer2 ACL rules, first need to create one Layer2 ACL and specify ACL type number to be from 1 to 1000.

Process

According to different destination, please execute corresponding steps. Refer to the following table.

Objective	Procedure
Create one layer2 ACL	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **filter-list** *acl-number* to create one layer2 ACL and enter Layer2 ACL Configuration View; 3. End.
Configure layer2 ACL rule	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **filter-list** *acl-number* to enter Layer2 ACL Configuration View; 3. Use the following commands to configure ACL rule matching MAC (user chooses the following commands according to your need); **filter** filter number **mac (**src-mac-address/M**|any) (**dst-mac-address/M

Objective	Procedure
	|any) **filter** filter number **src-mac** src-mac-address **src-mask** src-mac-mask **dst-mac** dst-mac-address **dst-mask** dst-mac-mask filter *filter number* mac (*src-mac-address/M*|any) (*dst-mac-address/M* |any) (customer|provider)(any|<1-4094>|<1-4094>/<1-4094>) (any|<0-7>) filter *filter number* src-mac *src-mac-address* src-mask *src-mac-mask* dst-mac *dst-mac-address* dst-mask *dst-mac-mask* (customer|provider) (any|<1-4094>|<1-4094>/<1-4094>) (any|<0-7>) filter *filter number* mac (*src-mac-address/M*|any) (*dst-mac-address/M* |any) eth-type (ip|arp|<0x1-0xfffe>) filter *filter number* src-mac *src-mac-address* src-mask *src-mac-mask* dst-mac *dst-mac-address* dst-mask *dst-mac-mask* eth-type (ip|arp|<0x1-0xfffe>) filter *filter number* mac (*src-mac-address/M*|any) (*dst-mac-address/M* |any) provider (any|<1-4094>) (any|<0-7>) customer (any|<1-4094>)(any|<0-7>) filter *filter number* mac (*src-mac-address/M*|any) (*dst-mac-address/M* |any) provider (<1-4094>/<1-4094>) (any|<0-7>) customer (any|<1-4094>)(any|<0-7>) filter *filter number* mac (*src-mac-address/M*|any) (*dst-mac-address/M* |any) provider (any|<1-4094>) (any|<0-7>) customer (<1-4094>/<1-4094>) (any|<0-7>) filter *filter number* src-mac(*src-mac-address/M*|any) src-mask *src-mac-mask* dst-mac *dst-mac-address* dst-mask *dst-mac-mask* provider (any|<1-4094>) (any|<0-7>) customer (any|<1-4094>)(any|<0-7>) filter *filter number* src-mac (*src-mac-address/M*|any) src-mask *src-mac-mask* dst-mac *dst-mac-address* dst-mask *dst-mac-mask* provider (<1-4094>/<1-4094>) (any|<0-7>) customer (any|<1-4094>)(any|<0-7>) filter *filter number* src-mac (*src-mac-address/M*|any) src-mask *src-mac-mask* dst-mac *dst-mac-address* dst-mask *dst-mac-mask* provider (any|<1-4094>) (any|<0-7>) customer (<1-4094>/<1-4094>)(any|<0-7>) filter *filter number* mac (*src-mac-address/M*|any) (*dst-mac-address/M* |any) provider (any|<1-4094>|<1-4094>/<1-4094>) (any|<0-7>) isid (any|<1-16777215>) filter *filter number* src-mac (*src-mac-address/M*|any) src-mask *src-mac-mask* dst-mac *dst-mac-address* dst-mask *dst-mac-mask* provider (any|<1-4094>|<1-4094>/<1-4094>) (any|<0-7>) isid

Objective	Procedure
	(any|<1-16777215>) 4. End.
Configure layer2 ACL action	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **filter-list** *acl-number* to enter Layer2 ACL Configuration View; 3. Use the following commands to configure ACL action; filter *rule-number* action { permit | deny } filter *rule-number* action redirect cpu filter *rule-number* action mirror cpu filter *rule-number* action mirror group *group-number* filter *rule-number* action redirect **{ fastethernet | eth-trunk }** *slot/port* filter *rule-number* action redirect eth-trunk *trunk number* filter *rule-number* action redirect ip-nexthop *ip-address* **filter** *rule-number* **action redirect ip-multihop** *ip-address ip-address* **filter** rule-number **action redirect ip-multihop** ip-address ip-address ip-address **filter** rule-number **action redirect ip-multihop** ip-address ip-address ip-address ip-address filter *rule-number* action { insert-outer-vid | replace-outer-vid } *vlan-id* filter *rule-number* action { insert-inner-vid | replace-inner-vid | remove-inner-vid } filter *rule-number* action vfp { insert-inner-vid | replace-inner-vid |insert-outer-vid | replace-outer-vid| deny | remove-inner-vid } *Vlan ID* filter *rule-number* action vfp filter *rule-number* action { cos | precedence | outer-tag-priority | inner-tag-priority } *priority-value* filter *rule-number* action { outer-tag-priority|inner-tag-priority } *Priority-value* filter *rule-number* action outer-tag-priority inner-tag-priority filter *rule-number* action dscp *dscp* filter *rule-number* action { precedence-priority | priority-precedence } **filter** rule-number **action counter** counter number 4. End.
Bind layer2 ACLL	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **filter-list global** { **in | out** } *acl-number* to globally bind designated ACL; 3. or use command of **filter-list** *acl-number* to enter Layer2 ACL Configuration View and then Use command of **filter-list** { **in** | **out** } *acl-number* to apply ACL to physical interface, trunk interface or VLAN interface;

Objective	Procedure
	4. End.

Attached List:

Parameter	Description	Value
acl-number	Access Control List number	to be from 1 to 4000 <1-1000>: layer2 ACL <1001-2000>: IPv4ACL <2001-3000>: Mixed ACL <3001-4000>: IPv6ACL
rule-number	rule number of ACL	to be from 1 to 16384
src-mac-address/M| **any**	source MAC information of ACL rule	*M* to be integer with range of from 1 to 24 **any** means any source MAC address
dst-mac-address/M |**any**	destination MAC information of ACL rule	*M* to be integer with range of from 1 to 24 **any** means any destination MAC address
src-mac-mask	source MAC mask of ACL rule	dotted decimal
dst-mac-mask	destination MAC mask of ACL rule	dotted decimal
provider (<1-4094>/<1-4094>) (any|<0-7>) customer (any|<1-4094>)(any|<0-7>)	VID/VID range or any both all	-
rule-number	rule number of ACL	to be from 1 to16384
VLAN ID	VLAN ID	to be from 1 to 4094

7.2.3 Configure Layer3 ACL

Background Information

One ACL is composed of some rules and actions.

Before configuring Layer3 ACL rules, first need to create one Layer3 ACL and specify ACL type number to be from 1001 to 2000.

Process

According to different destination, please execute corresponding steps. Refer to the following table.

Objective	Procedure
Create one layer3 ACL	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **filter-list** *acl-number* to create one layer3 ACL and enter Layer3 ACL Configuration View; 3. End.
Configure layer3 ACLrule	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **filter-list** *acl-number* to enter Layer3 ACL Configuration View; [User can choose from step3 to step8 to configure according to your need.] 3. (Optional) Use the following commands to configure ACL rule matching IP; **filter** rule-number **ip** { src-ip-address/M | **any**} { dst-ip-address/M | **any** } **filter** rule-number **src-ip** {src-ip-address | **any**} **src-mask** {src-ip-mask | **any**} **dst-ip** {dst-ip-address | **any**} **dst-mask** {dst-ip-mask | **any**} **filter** rule-number **ip** { src-ip-address/M | **any**} { dst-ip-address/M | **any** } **precedence** tos-priority **filter** rule-number **src-ip** { src-ip-address | any} **src-mask** {src-ip-mask | any} **dst-ip** {dst-ip-address | any} **dst-mask** {dst-ip-mask | any} **precedence** tos-priority **filter** rule-number **ip** { src-ip-address/M | **any**} { dst-ip-address/M | **any** } **dscp** dscp **filter** rule-number **src-ip** { src-ip-address | any} **src-mask** {src-ip-mask | any} **dst-ip** {dst-ip-address | any} **dst-mask** {dst-ip-mask | any} **dscp** dscp **filter** rule-number **ip** { src-ip-address/M | **any**} { dst-ip-address/M | **any** } **fragment** **filter** rule-number **src-ip** { src-ip-address | any} **src-mask** {src-ip-mask | any} **dst-ip** {dst-ip-address | any} **dst-mask** {dst-ip-mask | any} **fragment** **filter** filter number **ip** (src-ip-address/M **|any)** (dst-ip-address M**|any) precedence** tos field **fragment** **filter** filter number **src-ip** { src-ip-address | any} **src-mask** {src-ip-mask | any} **dst-ip** {dst-ip-address | any} **dst-mask** {dst-ip-mask | any} **precedence** tos field **fragment** filter *filter number* ip (*src-ip-address/M* |any) (*dst-ip-address M* |any)

Objective	Procedure
	dscp (*dscp field*|af11|af12|af13|af21|af22|af23|af31|af32|af33|af41|af42|af43|cs1|cs2|cs3|cs4|cs5|cs6|cs7|default|ef) fragment filter *filter number* src-ip *{ src-ip-address* | *any}* src-mask {*src-ip-mask* | *any}* dst-ip {*dst-ip-address* | *any}* dst-mask *{dst-ip-mask* | *any}* dscp(*dscp field* |af11|af12|af13|af21|af22|af23|af31|af32|af33|af41|af42|af43|cs1|cs2|cs3|cs4|cs5|cs6|cs7|default|ef) fragment **filter** filter number **ip (**src-ip-address/M **|any) (**dst-ip-address M **|any) proto-type** proto-type field **filter** filter number **src-ip** { src-ip-address | any} **src-mask {**src-ip-mask | any} **dst-ip {**dst-ip-address | any} **dst-mask** {dst-ip-mask | any} **proto-type** proto-type field **filter** filter number **ip (**src-ip-address/M **|any) (**dst-ip-address M **|any) ttl** ttl field **filter** filter number **src-ip** { src-ip-address | any} **src-mask {**src-ip-mask | any} **dst-ip {**dst-ip-address | any} **dst-mask** {dst-ip-mask | any} **ttl** ttl field 4. (Optional) Use the following commands to configure ACL rule matching TCP; filter *filter number* tcp (*src-ip-address/M* |any) (<0-65535>|<0-65535>/<0-65535>|any) (*dst-ip-address/M* |any) (<0-65535>|<0-65535>/<0-65535>|any) **filter** filter number **tcp src-ip** { src-ip-address | any} **src-mask** src-ip-mask **(<0-65535>|any) dst-ip** { src-ip-mask | any} **dst-mask** dst-ip-mask **(<0-65535>|any)** filter *filter number* tcp (*src-ip-address/M* |any) (<0-65535>|<0-65535>/<0-65535>|any) (*dst-ip-address/M* |any) (<0-65535>|<0-65535>/<0-65535>|any) fragment (syn|synack|ack|fin|finack|psh|rst|urg|*field*|) filter *filter number* tcp src-ip *{ src-ip-address* | *any}* src-mask *src-ip-mask* (<0-65535>|any) dst-ip*dst-ip-addres* dst-mask *dst-ip-mask* (<0-65535>|any)(syn|synack|ack|fin|finack|psh|rst|urg| *field*|) fragment 5. (Optional) Use the following commands to configure ACL rule matching ICMP; **filter** filter number **icmp (**src-ip-address/M **|any) (**dst-ip-address M **|any)** **filter** filter number **icmp src-ip** { src-ip-address | any} **src-mask** { src-ip-mask | any} **dst-ip** src-ip-mask **dst-mask** { dst-ip-mask } **filter** filter number **icmp (**src-ip-address/M **|any) (**dst-ip-address M

Objective	Procedure
	|any) (icmp type**|any) (**icmp code**|any)** **filter** filter number **icmp src-ip** src-ip-address **src-mask** {src-ip-mask | any} **dst-ip** src-ip-mask **dst-mask** dst-ip-mask icmp type **(**icmp code **|any)** 6. (Optional) Use the following commands to configure ACL rule matching IGMP; **filter** filter number **igmp (**src-ip-address/M **|any) (**dst-ip-address M **|any)** **filter** filter number **igmp src-ip** src-ip-address **src-mask** src-ip-mask **dst-ip** src-ip-mask **dst-mask** dst-ip-mask 7. (Optional) Use the following commands to configure ACL rule matching UDP; filter *filter number* udp (*src-ip-address/M* |any) (<0-65535>|<0-65535>/<0-65535>|any) (*dst-ip-address/M* |any) (<0-65535>|<0-65535>/<0-65535>|any)|fragment filter *filter number* udp src-ip *{ src-ip-address | any}* src-mask *src-ip-mask* (<0-65535>|any) dst-ip *{ src-ip-mask | any}* dst-mask {*dst-ip-mask* | *any}* (<0-65535>|any) |fragment 8. (Optional) Use the following commands to configure ACL rule matching ARP; filter *filter number* arp (request|response|any) (*src-ip-address/M* |any) (*dst-ip-address/M* |any) filter filter number arp (request|response|any) src-ip src-ip-address src-mask { src-ip-mask | any} dst-ip src-ip-mask dst-mask dst-ip-mask 9. End.
Configure layer3 ACL action	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **filter-list** *acl-number* to enter Layer3 ACL Configuration View; 3. Use the following commands to configure ACL action; filter *rule-number* action { permit | deny } filter *rule-number* action redirect cpu filter *rule-number* action mirror cpu filter *rule-number* action mirror group *group-number* filter *rule-number* action redirect **{ fastethernet | eth-trunk }** *slot/port* filter *rule-number* action redirect eth-trunk *trunk number* filter *rule-number* action redirect ip-nexthop *ip-address* **filter** *rule-number* **action redirect ip-multihop** *ip-address ip-address* **filter** rule-number **action redirect ip-multihop** ip-address ip-address ip-address **filter** rule-number **action redirect ip-multihop** ip-address ip-address

Objective	Procedure
	ip-address ip-address filter *rule-number* action { insert-outer-vid | replace-outer-vid } *vlan-id* filter *rule-number* action { insert-inner-vid | replace-inner-vid | remove-inner-vid } filter *rule-number* action vfp { insert-inner-vid | replace-inner-vid |insert-outer-vid | replace-outer-vid| deny | remove-inner-vid } *Vlan ID* filter *rule-number* action vfp filter *rule-number* action { cos | precedence | outer-tag-priority | inner-tag-priority } *priority-value* filter *rule-number* action { outer-tag-priority|inner-tag-priority } *Priority-value* filter *rule-number* action outer-tag-priority inner-tag-priority filter *rule-number* action dscp *dscp* filter *rule-number* action { precedence-priority | priority-precedence } **filter** rule-number **action counter** counter number 4. End.
Bind layer3 ACL	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **filter-list global** { **in | out** } *acl-number* to bind designated ACL globally; 3. or use command of **filter-list** *acl-number* to enter layer3 ACL Configuration View and then Use command of **filter-list** { **in** | **out** } *acl-number* to apply ACL to physical interface, trunk interface and VLAN interface; 4. End.

Attached List:

Parameter	Description	Value
acl-number	Access Control List	to be from 1 to 4000 <1-1000>: layer2 ACL <1001-2000>: IPv4ACL <2001-3000>: Mixed ACL <3001-4000>: IPv6ACL
rule-number	rule number of ACL	to be from 1 to 16384
src-ip-address/M | **any**	source IP address information of ACL rule	*src-ip-address* is dotted decimal, *M* is from 1 to 24 **any** means any source IP address
dst-ip-address/M | **any**	destination IP address of ACL rule	*dst-ip-address* is dotted decimal, *M* is from 1 to 24 **any** means any destination IP address
src-ip-mask| **any**	Source IP address mask	dotted decimal

Parameter	Description	Value
	information of ACL rule	
dst-ip-mask| **any**	Destination IP address mask information of ACL rule	dotted decimal
tos-priority	Priority of TOS segment	to be from 0 to 7
dscp	DSCP value	using integer with range of from 0 to 63 using name, to be key word of af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, default or ef
tos field	ToS segment of ACL rule	to be from 0 to 7
fragment	Whether the rule is effective for non-head fragment message	-
proto-type field	protocol type segment of ACL rule	to be from 1 to 255
ttl field	TTL segment of ACL rule	to be from 1 to 255

7.2.4 Configure Mixed ACL

Background Information

One ACL is composed of some rules and actions.

Before configuring Mixed ACL rules, first need to create one Mixed ACL and specify ACL type number to be from 2001 to 3000.

Process

According to different destination, please execute corresponding steps. Refer to the following table.

Objective	Procedure
Create one mixed ACL	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **filter-list** *acl-number* to create one mixed ACL and enter Mixed ACL Configuration View; 3. End.
Configure mixed ACL rule	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **filter-list** *acl-number* to enter Mixed ACL Configuration View; 3. Under mixed mode, user can configure layer2 and layer3 ACL rule, please refer to 7.2.2 and 7.2.3 of this manual;

Objective	Procedure
	4. End.
Configure mixed ACL action	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **filter-list** *acl-number* to enter Mixed ACL Configuration View; 3. Use the following commands to configure ACL action; filter *rule-number* action { permit | deny } filter *rule-number* action redirect cpu filter *rule-number* action mirror cpu filter *rule-number* action mirror group *group-number* filter *rule-number* action redirect **{ fastethernet | eth-trunk }** *slot/port* filter *rule-number* action redirect eth-trunk *trunk number* filter *rule-number* action redirect ip-nexthop *ip-address* **filter** *rule-number* **action redirect ip-multihop** *ip-address ip-address* **filter** rule-number **action redirect ip-multihop** ip-address ip-address ip-address **filter** rule-number **action redirect ip-multihop** ip-address ip-address ip-address ip-address filter *rule-number* action { insert-outer-vid | replace-outer-vid } *vlan-id* filter *rule-number* action { insert-inner-vid | replace-inner-vid | remove-inner-vid } filter *rule-number* action vfp { insert-inner-vid | replace-inner-vid |insert-outer-vid | replace-outer-vid| deny | remove-inner-vid } *Vlan ID* filter *rule-number* action vfp filter *rule-number* action { cos | precedence | outer-tag-priority | inner-tag-priority } *priority-value* filter *rule-number* action { outer-tag-priority|inner-tag-priority } *Priority-value* filter *rule-number* action outer-tag-priority inner-tag-priority filter *rule-number* action dscp *dscp* filter *rule-number* action { precedence-priority | priority-precedence } **filter** rule-number **action counter** counter number 4. End.
Bind mixed ACL	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **filter-list global** { **in | out** } *acl-number* to bind globally to designated ACL; 3. or use command of **filter-list** *acl-number* to enter Mixed ACL Configuration View and then Use command of **filter-list** { **in** | **out** } *acl-number* to apply ACL to physical interface, trunk interface and VLAN interface; 4. End.

Attached List:

Parameter	Description	Value
acl-number	Access Control List	to be from 1 to 4000 <1-1000>: layer2 ACL <1001-2000>: IPv4ACL <2001-3000>: mixed ACL <3001-4000>: IPv6ACL
rule-number	Rule number of ACL	to be from 1 to 16384
src-mac-address/M| **any**	Source MAC address information of ACL rule	*M* is integer with range of from 1 to 24 **any** means any source MAC address
dst-mac-address/M |**any**	Destination MAC address information of ACL rule	*M* is integer with range of from 1 to 24 **any** means any destination MAC address
src-mac-mask	Source MAC address mask information of ACL rule	dotted decimal
dst-mac-mask	Destination MAC address mask information of ACL rule	dotted decimal
provider (<1-4094>/<1-4094>) (any|<0-7>) customer (any|<1-4094>)(any|<0-7>)	VID/VID range or both of them	-
rule-number	Rule number of ACL	to be from 1 to 16384
VLAN ID	VLAN ID	to be from 1 to 4094

7.2.5 Configure Layer3 ACL6

Background Information

One ACL is composed of some rules and actions.

Before configuring Layer3 ACL6 rules, first need to create one Layer3 ACL6 and specify ACL type number to be from 3001 to 4000.

Process

According to different destination, please execute corresponding steps. Refer to the following table.

Objective	Procedure
Create one layer3 ACL6	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **filter-list** *acl-number* to create one layer3 ACL6 and enter Layer3 ACL6 Configuration View; 3. End.
Configure layer3 ACL6 rule	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **filter-list** *acl-number* to enter Layer3 ACL6 Configuration View; [User can choose from step3 to step8 to configure according your need.] 3. (Optional) Use the following commands to configure ACL rule matching IPv6; **filter** rule-number **ip6** { src-ip6-address/M | **any**} { dst-ip6-address/M | **any** } **filter** rule-number **ip6** { src-ip6-address/M | **any**} { dst-ip6-address/M | **any** } **next-header** next-header value **filter** rule-number **ip6** { src-ip6-address/M | **any**} { dst-ip6-address/M | **any** } **hop-limit** hop-limit value 4. (Optional) Use the following commands to configure ACL rule matching TCP6; filter *filter number* tcp6 (*src-ip6-address/M* |any) (<0-65535>|<0-65535>/<0-65535>|any) (*dst-ip6-address/M* |any) (<0-65535>|<0-65535>/<0-65535>|any) filter *filter number* tcp6 (*src-ip6-address/M* |any) (<0-65535>|<0-65535>/<0-65535>|any) (*dst-ip6-address/M* |any) (<0-65535>|<0-65535>/<0-65535>|any) (syn|synack|ack|fin|finack|psh|rst|urg|*field*) fragment 5. (Optional) Use the following commands to configure ACL rule matching ICMP6; **filter** filter number **icmp6 (**src-ip6-address/M **|any) (**dst-ip6-address M **|any)** **filter** filter number **icmp6 (**src-ip6-address/M **|any) (**dst-ip6-address M **|any) (**icmp type**|any) (**icmp code**|any)** 6. (Optional) Use the following commands to configure ACL rule matching IGMP6; **filter** filter number **igmp6 (**src-ip6-address/M **|any) (**dst-ip6-address M **|any)** 7. (Optional) Use the following commands to configure ACL rule matching UDP6; filter *filter number* udp6 (*src-ip6-address/M* |any) (<0-65535>|<0-65535>/<0-65535>|any) (*dst-ip6-address/M* |any)

Objective	Procedure
	(<0-65535>|<0-65535>/<0-65535>|any) fragment 8. (Optional) Use the following commands to configure ACL rule matching ARP6; filter *filter number* arp6 (request|response|any) (*src-ip6-address/M* |any) (*dst-ip6-address/M* |any) 9. End.
Configure layer3 ACL6 action	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **filter-list** *acl-number* to enter Layer3 ACL6 Configuration View; 3. Use the following commands to configure ACL action; filter *rule-number* action { permit | deny } filter *rule-number* action redirect cpu filter *rule-number* action mirror cpu filter *rule-number* action mirror group *group-number* filter *rule-number* action redirect **{ fastethernet | eth-trunk }** *slot/port* filter *rule-number* action redirect eth-trunk *trunk number* filter *rule-number* action redirect ip-nexthop *ip-address* **filter** *rule-number* **action redirect ip-multihop** *ip-address ip-address* **filter** rule-number **action redirect ip-multihop** ip-address ip-address ip-address **filter** rule-number **action redirect ip-multihop** ip-address ip-address ip-address ip-address filter *rule-number* action { insert-outer-vid | replace-outer-vid } *vlan-id* filter *rule-number* action { insert-inner-vid | replace-inner-vid | remove-inner-vid } filter *rule-number* action vfp { insert-inner-vid | replace-inner-vid |insert-outer-vid | replace-outer-vid| deny | remove-inner-vid } *Vlan ID* filter *rule-number* action vfp filter *rule-number* action { cos | precedence | outer-tag-priority | inner-tag-priority } *priority-value* filter *rule-number* action { outer-tag-priority|inner-tag-priority } *Priority-value* filter *rule-number* action outer-tag-priority inner-tag-priority filter *rule-number* action dscp *dscp* filter *rule-number* action { precedence-priority | priority-precedence } **filter** rule-number **action counter** counter number 4. End.
Bind layer3 ACL6	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **filter-list global** { **in | out** } *acl-number* to bind globally to designated ACL;

Objective	Procedure
	3. or use command of **filter-list** *acl-number* to enter Layer3 ACL6 Configuration View and then Use command of **filter-list** { **in** | **out** } *acl-number* to apply ACL6 to physical interface, trunk interface and VLAN interface; 4. End.

Attached List:

Parameter	Description	Value
acl-number	Access Control List	to be from 1 to 4000 <1-1000>: layer2 ACL <1001-2000>: IPv4ACL <2001-3000>: Mixed ACL <3001-4000>: IPv6ACL
rule-number	Rule number of ACL	to be from 1 to 16384
src-ip6-address/M | **any**	Source IP address of ACL rule	*src-ip6-address* is dotted hex, form as X:X::X:X, *M* to be from 1 to 128 **any** means any source IP address
dst-ip6-address/M | **any**	Destination IP address of ACL rule	*dst-ip6-address* is dotted hex, form as X:X::X:X, *M* to be from 1 to 128 **any** means any destination IP address
next-header value	next message head value	to be from 1 to 255
hop-limit value	hop limitation value	to be from 1 to 255
icmp type	ICMP range of ACL rule	to be from 1 to 255
Icmp code	ICMP code range of ACL rule	to be from 1 to 255
(<0-65535>|<0-65535>/<0-65535>|any)	destination port/port range	-
field	Segment range, including syn, synack, ack, fin, finack, psh, rst and urg segment	to be from 0 to 63
fragment	Whether the rule is effective for non first fragment message	-
(request|response|any)	ARP request message/response message	-

Parameter	Description	Value
	or any both	

7.2.6 Configure ACL Optional Function

Background Information

ACL optional function includes:

- Create ACL effective time period

  After creating ACL effective time period, when configuring ACL rule to refer to this time period, the ACL rule is effective during the period; If configure the rule not refer to this time period, the ACL rule is not subjected to the time limits unless deleting the ACL.

- Create ACL rate limitation template

  After creating ACL rate limitation template, when configuring ACL rule to bind with rate limitation template, the ACL rule can be used to filter data according to different rate limitation rule.

- Create ACL counting template

  After creating ACL counting template, when configuring ACL rule to bind with counting template, the ACL rule can be used to count data for statistic according to different counting type.

Purpose

According to the real condition, configuring ACL optional function can provide variety methods to filter data packet for user.

Process

According to different destination, please execute corresponding steps. Refer to the following table.

Objective	Procedure
Creante ACL effective time period	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **time-range list** *LIST-NUMBER* to enter Time-range Configuration View; 3. Use the following commands to configure the absolute start and end time of time-range module;

Objective	Procedure
	time-range RANGE-NUMBER **absolute from** hh:mm:ss YY/MM/DD or **time-range** RANGE-NUMBER **absolute from** hh:mm:ss YY/MM/DD **to** hh:mm:ss YY/MM/DD; 4. Use command of **time-range** *RANGE-NUMBER* **everyday** *hh:mm:ss* **to** *hh:mm:ss* to configure everyday time range of time-range module; 5. Use command of **time-range** *RANGE-NUMBER* **everyhour** *mm:ss* **to** *mm:ss* to configure every hour range of time-range module; 6. Use command of **time-range** *RANGE-NUMBER* **everymonth** *hh:mm:ss MM* **to** *hh:mm:ss MM* to configure every month range of time-range module; 7. Use command of **time-range** *RANGE-NUMBER* **everyweek** *hh:mm:ss (mon|tue|wed|thu|fri|sat|sun)* **to** *hh:mm:ss (mon|tue|wed|thu|fri|sat|sun)* to configure every week range of time-range module; 8. Use command of **time-range** *RANGE-NUMBER* **everyweekday** *hh:mm:ss* **to** *hh:mm:ss* to configure weekday range of time-range module; 9. Use command of **time-range** *RANGE-NUMBER* **everyweekend** *hh:mm:ss* **to** *hh:mm:ss* to configure weekend range of time-range module; 10. Use command of **time-range** *RANGE-NUMBER* **everyyear** *hh:mm:ss MM/DD* **to** *hh:mm:ss MM/DD* to configure every year range of time-range module; 11. Use command of **quit** to exit to Global Configuration View; 12. Use command of **filter-list** *acl-number* to enter ACL Configuration View; 13. Use command of **time-range list** *time-range acl-number* to bind time range module with ACL; 14. End.
Create ACL rate limitation template	1. Use command of **configure** to enter Global Configuration View; 2. Use the following commands to configure Meter template; **meter** meter-number **cir** CIR-number **cbs** CBS-number **ebs** EBS-number **meter** meter-number **cir** CIR-number **cbs** CBS-number **ebs** EBS-number **(aware|blind)** **meter** meter-number **cir** CIR-number **cbs** CBS-number **pbs** PBS-number **pir** PIR number **meter** meter-number **cir** CIR-number **cbs** CBS-number **pbs** PBS-number **pir** PIR number **(aware|blind)** 3. Use command of **filter-list** *acl-number* to enter ACL Configuration View; 4. Use command of **filter** *rule-number* **meter** *meter-number* to bind ACL rule with one meter template; 5. Use the following commands to configure how to deal with the coloring packet according to rate limitation template;

Objective	Procedure
	filter *rule-number* outaction { red | yellow } drop filter *rule-number* outaction { red | yellow } remark-dscp *dscp* filter *rule-number* outaction { red | yellow } remark-dot1p *priority* filter *rule-number* car *car-value* outaction drop 6. End.
Create ACL counting template	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **counter** counter-number **(packet/byte|all)** **sort** (green/red/greenred/greenyellow/redyellow|**total**) to configure counter template; 3. Use command of **filter-list** *acl-number* to enter ACL Configuration View; 4. Use command of **filter** *rule-number* **action counter** *counter-number* to bind counting template with ACL; 5. End.

Attached List:

Parameter	Description	Value
LIST-NUMBER	time-range module list name	to be from 1 to 128
RANGE-NUMBER	Range number	to be from 1 to 16
hh:mm:ss	Start or end time(hour:minute:second)	to be <0-23>:<0-59>:<0-59>
YY/MM/DD	Start or end time(year/month/day)	to be <2000-2100>:<1-12>:<1-31>
mm:ss	Start or end time(minute:second)	to be <0-59>:<0-59>
MM	Month	to be from 1 to 31
(mon|tue|wed|thu|fri|sat|sun)	Week	-
MM/DD	Start or end time(month/day)	to be <1-12>:<1-31>
acl-number	Access Control List	to be from 1 to 4000 <1-1000>: layer2 ACL <1001-2000>: IPv4ACL <2001-3000>: Mixed ACL <3001-4000>:IPv6ACL
meter number	Meter number	to be from 1 to 256
CIR number	CIR item number	to be from 8 to 4294967295
CBS number	CBS item number	to be from 10000 to 4294967295
EBS number	EBS item number	to be from 10000 to 4294967295

Parameter	Description	Value
PBS number	PBS item number	to be from 10000 to 4294967295
PIR number	PIR item number	to be from 8 to 4294967295
aware	response to rate limited rule and coloring rule	-
blind	Not to response to rate limited rule and coloring rule	-
counter number	counter number	to be from 1 to 1024
packet/byte|all	Data type, byte type of counter	-
green/red/greenred/greenyellow/redyellow|total	Display type of counter state, including green, red, green/red, green/yellow and red/yellow	-
red|yellow	Color of data packet	-
drop	to drop data packet	-
remark-dscp	to remark DSCP value	-
dscp	DSCP value	using integer with range of from 0 to 63 using name, to be key word of af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, default or ef
remark-dot1p	to remark 802.1p priority	-
priority	802.1p priority value of VLAN Tag	to be from 0 to 7

7.2.7 Maintenance and Debug

Purpose

When ACL function is abnormal, user can use this operation to check or debug.

Process

According to different destination, please execute corresponding steps. Refer to the following table.

Objective	Procedure
Clear ACL statistic	1. Use command of **configure** to enter Global Configuration View; 2. Use the following commands to remark ACL filter counter;

Objective	Procedure
information	reset counter filte-list *acl-number* filter *filter-number* { in | out } reset counter filte-list *acl-number* filter *filter-number* port fastethernet *slot-number port-number* { in | out } reset counter filte-list *acl-number* filter *filter-number* port eth-trunk *trunk-number* { in | out } reset counter filte-list *acl-number* filter *filter-number* vlan *VLANID* { in | out } 3. End.
Delete ACL action	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **filter-list** *acl-number* to enter ACL Configuration View; 3. Use command of **no filter** *rule-number* **action** to delete ACL corresponding action; 4. End.
Delete ACL rule	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **filter-list** *acl-number* to enter ACL Configuration View; 3. Use command of **no filter** *rule-numbe* to delete ACL rule; 4. End.
Check ACL configuration information	1. Use command of **disable** to exit Normal User View; or use command of **configure** to enter Global Configuration View; or use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter Interface Configuration View; or use command of **filter-list** *acl-number* to enter ACL Configuration View, or no use any command to keep current Privileged User View; 2. Use command of **show filter-list** or **show filter-list** *acl-number* to display ACL configuration information; 3. End.
Check ACL configuration file information	1. Use command of **disable** to exit Normal User View; or use command of **configure** to enter Global Configuration View; or use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter Interface Configuration View; or use command of **filter-list** *acl-number* to enter ACL Configuration View, or no use any command to keep current Privileged User View; 2. Use command of **show filter-list config** to display ACL configuration file information; 3. End.
Check ACL statistic information	1. Use command of **disable** to exit Normal User View; or use command of **configure** to enter Global Configuration View; or use command of **interface fastethernet** *interface-number* or **interface eth-trunk**

Objective	Procedure
	trunk-number to enter Interface Configuration View; or use command of **filter-list** *acl-number* to enter ACL Configuration View, or no use any command to keep current Privileged User View; 2. Use command of **show filter-list statistic** to display ACL statistic information; 3. End.
Check information of interface applied ACL	1. Use command of **disable** to exit Normal User View; or use command of **configure** to enter Global Configuration View; or use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter Interface Configuration View; or use command of **filter-list** *acl-number* to enter ACL Configuration View, or no use any command to keep current Privileged User View; 2. Use command of **show filter-list interface** to display information of interface applied ACL; 3. End.
Check ACL global configuration information	1. Use command of **disable** to exit Normal User View; or use command of **configure** to enter Global Configuration View; or use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter Interface Configuration View; or use command of **filter-list** *acl-number* to enter ACL Configuration View, or no use any command to keep current Privileged User View; 2. Use command of **show filter-list global** to display ACL global configuration information; 3. End.
Check statistic table information and configuration information	1. Use command of **disable** to exit Normal User View; or use command of **configure** to enter Global Configuration View; or no use any command to keep current Privileged User View; 2. Use command of **show counter config** or **show counter** *counter-id* or **show counter** to display statistic table information and configuration information; 3. End.

Attached List:

Parameter	Description	Value
acl-number	Access Control List	to be from 1 to 4000
counter-id	Statistic table ID	to be from 1 to 1024

7.2.8 Example

7.2.8.1 Configure Layer2 ACL

Network Requirements

Switch is used as gateway, connecting with user PC. Require to configure ACL to deny message with source MAC of 0001-0203-0405 and destination MAC of 0102-0304-0506 to pass.

Network Diagram

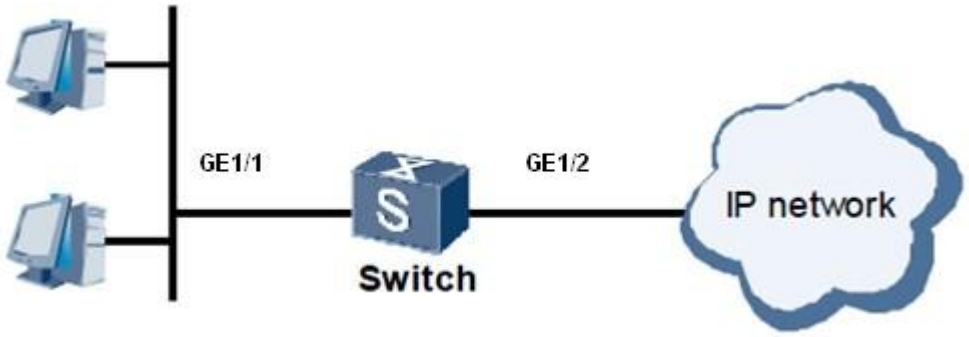


Figure Layer2 ACL Topology

Configuration Steps

1. Create layer2 ACL.

Switch#configure

Switch(config)#filter-list 1

Switch(configure-filter-l2-1)#

2. Configure layer2 ACL rule.

Switch(configure-filter-l2-1)#filter 1 mac 00:01:02:03:04:05/48 01:02:03:04:05:06/48

3. Configure layer2 ACL action.

Switch(configure-filter-l2-1)#filter 1 action deny

4. Binding ACL to interface.

Switch(configure-filter-l2-1)#quit

Switch(config)#interface fastethernet 1/0/1

Switch(config-ge1/0/1)#filter-list in 1

7.2.8.2 Configure Layer3 ACL

Network Requirements

Every department of the corporate network are connected with each other by Switch. Require to configure IPv4 ACL to deny „Research & Development Dept.‟ to access salary query server (with IP address of 10.164.9.9) at time of 8:30 to 17:30. But the president office can access salary query server at any time without limitation.

Network Diagram

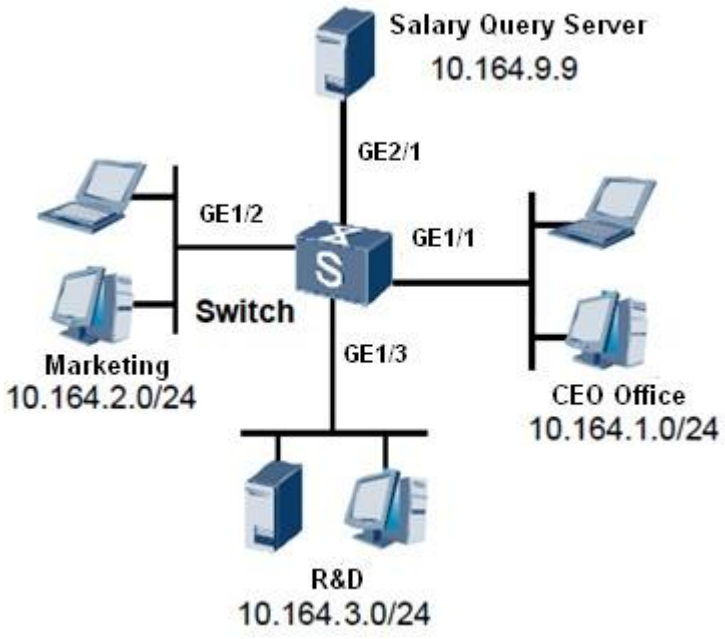


Figure Layer3 ACL Topology

Configuration Steps

1. Configure time-range.

Switch#configure

Switch(config)#time-range list 1

Switch(config-timerange1)#time-range 1 everyweekday 8:30:00 to 17:30:00

Switch(config-timerange1)#quit

2. Configure ACL to allow president office to access salary query server.

Switch(config)# filter-list 1001

Switch(configure-filter-ipv4-1001)#filter 1 ip 10.164.1.0/24 10.164.9.9/32

Switch(configure-filter-ipv4-1001)#filter 1 action permit

Switch(configure-filter-ipv4-1001)#quit

3. Configure ACL to deny Market Dept to access salary query server.

Switch(config)#filter-list 1002

Switch(configure-filter-ipv4-1002)#filter 1 ip 10.164.2.0/24 10.164.9.9/32

Switch(configure-filter-ipv4-1002)#filter 1 action deny

4. Configure ACL to allow Market Dept to access salary query server at desigenated time interval.

Switch(configure-filter-ipv4-1002)#filter 1 time-range 1

Switch(configure-filter-ipv4-1002)#quit

5. Configure ACL to deny Research & Development Dept to access salary query server.

Switch(configure)# filter-list 1003

Switch(configure-filter-ipv4-1003)#filter 1 ip 10.164.3.0/24 10.164.9.9/32

Switch(configure-filter-ipv4-1003)#filter 1 action deny

6. Configure ACL to allow Research & Development Dept to access salary query server at desigenated time interval.

Switch(configure-filter-ipv4-1003)#filter 1 time-range 1

Switch(configure-filter-ipv4-1003)#quit

7. Apply ACL to interface.

Switch(config)#interface fastethernet 1/0/1

Switch(config-ge1/0/1)#filter-list in 1001

Switch(config-ge1/0/1)#quit

Switch(config)#interface fastethernet 1/0/2

Switch(config-ge1/0/2)#filter-list in 1002

Switch(config-ge1/0/2)#quit

Switch(config)#interface fastethernet 1/0/3

Switch(config-ge1/0/3)#filter-list in 1003

7.2.8.3 Configure Mixed ACL

Network Requirements

Switch is used as gateway, connecting with user PC. Require to configure ACL to send message with source MAC of 00:01:02:00:00:00/24 and source IP of 1:2:3:1/24 network segment to CPU.

Network Diagram

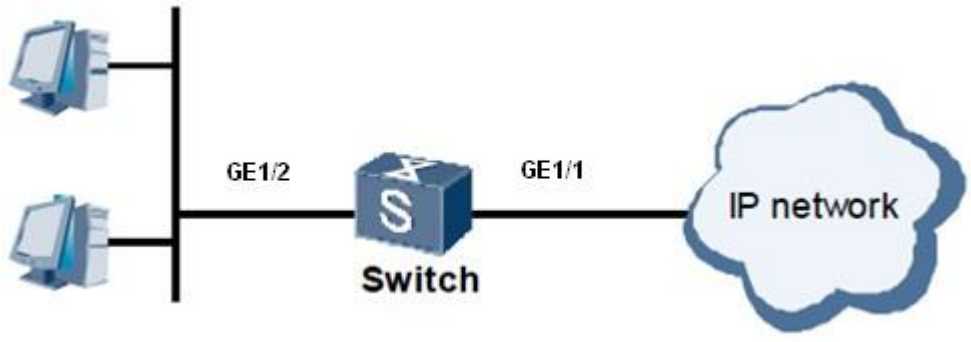


Figure Mixed ACL Topology

Configuration Steps

1. Create mixed ACL.

Switch#configure

Switch(config)#filter-list 2001

Switch(configure-filter-hybrid-2001)#

2. Configuer layer2 ACL rule.

Switch(configure-filter-hybrid-2001)#filter 1 mac 00:01:02:00:00:00/24 any eth-type any provider any any customer any any ip 1.2.3.1/24 any proto-type any

3. Configure layer2 ACL action.

Switch(configure-filter-hybrid-2001)#filter 1 action cpu

4. Apply ACL to interface.

Switch(configure-filter-hybrid-2001)#quit

Switch(config)#interface fastethernet 1/0/2

Switch(config-ge1/0/2)#filter-list in 2001

7.2.8.4 Configure Layer3 ACL6

Network Requirements

SwitchA is connected with SwitchB by GE interface. Configure ACL6 rule on SwitchA and deny message with source IPv6 address of 3001::2 to enter GE1/0/1 interface of SwitchA.

Network Diagram

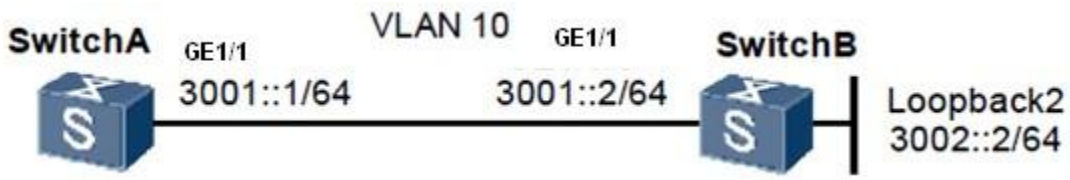


Figure Layer3 ACL6 Topology

Configuration Steps

1. Create layer3 ACL6.

Switch#configure

Switch(config)#filter-list 3001

Switch(configure-filter-ipv6-3001)#

2. Create layer3 ACL6 rule.

Switch(configure-filter-ipv6-3001)#filter 1 ip6 3001::2/64 any

3. Create layer3 ACL6 action.

Switch(configure-filter-ipv6-3001)#filter 1 ac deny

4. Bind ACL to interface GE1/0/1 of SwitchA ingress direction.

Switch(configure-filter-ipv6-3001)#quit

Switch(config)#interface fastethernet 1/0/1

Switch(config-ge1/0/1)#filter-list in 3001

7.2.8.5 Configure Rate Limitation Template

Network Requirements

Switch is used as gateway, connecting with user PC. Require to configure ACL to limit the rate of message received by Switch of interface GE1/0/2 with source MAC to be 0001-0203-0405, and modify the DSCP value of yellow message to be AF11. .

Network Diagram

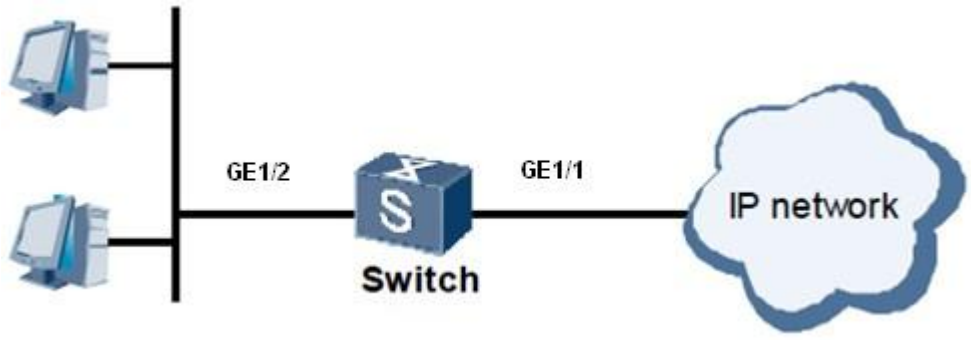


Figure Rate Limitation Template Topology

Configuration Steps

1. Configure rate limitation template.

Switch#configure

Switch(config)#meter 1 cir 64 cbs 10000 pbs 10000 pir 64

2. Create ACL.

Switch(config)#filter-list 1

Switch(configure-filter-l2-1)#

3. Configure ACL rule.

Switch(configure-filter-l2-1)#filter 1 mac 00:01:02:03:04:05/48 any

4. Bind rate limitation template with ACL.

Switch(configure-filter-l2-1)#filter 1 meter 1

5. Configure ACL action.

Switch(configure-filter-l2-1)#filter 1 outaction yellow remark-dscp af11

6. Apply ACL to interface.

Switch(configure-filter-l2-1)#quit

Switch(config)#interface fastethernet 1/0/2

Switch(config-ge1/0/2)#filter-list in 1

7.2.8.6 Configure Counting Template

Network Requirements

Switch is used as gateway, connecting with user PC. Require to configure ACL to count message number with source IP address to be 10.1.1.1/24 network segment received by SwitchA of interface GE1/0/2.

Network Diagram

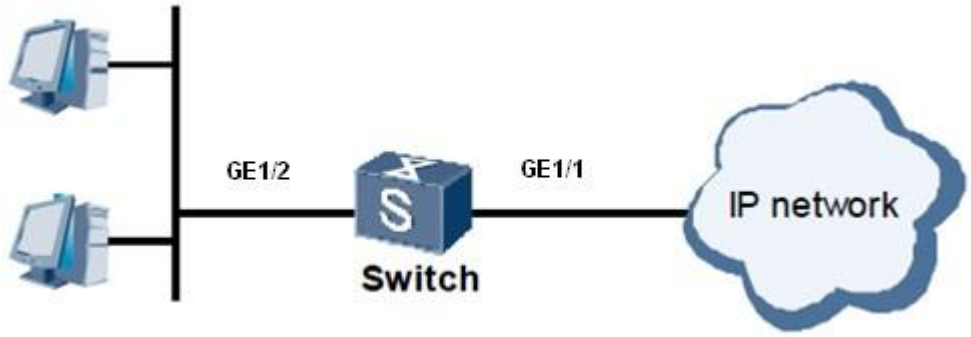


Figure Counting Template Topology

Configuration Steps

1. Configure counting template.

Switch#configure

Switch(config)# counter 1 packet sort total

2. Create ACL.

Switch(config)#filter-list 1001

Switch(configure-filter-ipv4-1001)#

3. Configure ACL rule.

Switch(configure-filter-ipv4-1001)#filter 1 ip 10.1.1.1/24 any

4. Bind counting template with ACL.

Switch(configure-filter-ipv4-1001)#filter 1 action counter 1

5. Apply ACL to interface.

Switch(configure-filter-ipv4-1001)#quit

Switch(config)#interface fastethernet 1/0/2

Switch(config-ge1/0/2)#filter-list in 1

Chapter8
Reliability Configuration

8.1 Summary

This chapter mainly introduces MSTP AND RLINK function of QSW-2870 in the network and affords the reliability configuration method.

This chapter includes the following section.

8.2 MSTP Configuration

8.2.1 STP Introduction

STP Generation Reason

The basic idea of STP protocol is very simple. There will be no loop of the tree grown in nature. And then STP defines the Root Bridge, Root Port, Designated Port, Path Cost and concepts like these. Its purpose is that it can cut out the redundant loops by constructing a tree and at the same time it can implement the link backup and path optimization. The algorithm used to construct the tree is called Spanning Tree Algorithm.

In order to implement the function, network bridges must have some information interaction with each other. These information interaction units are called BPDU (Bridge Protocol Data Unit). STP BPDU is a sort of Layer-2 message and its destination MAC is multicast address of 01-80-C2-00-00-00. All the bridges which support STP will receive and deal with the BPDU message. The data field of the message has all useful information used for calculating STP.

STP Working Process

Firstly carry out the root bridge election. The election basis is the bridge ID assembled by bridge priority and bridge MAC. The bridge with the smallest bridge ID will become the root bridge in the network. Its all ports are connected with the downstream Bridge. So the role of its port becomes the designated port. Next, the downstream bridge connected with the root bridge will respectively choose one “the most robust” branch as the path to the root bridge and the role of corresponding ports will become the root port. This process cycles to the network edge. After the designated port and the root port are confirmed, one tree is generated. After a period of time (default to be 30s), the STP is stable. The designated port and the root port are in the forwarding state and other ports are in blocking state. STP BPDU will be periodically sent out from the designated port of each bridge to maintain the link state. If the network topology changes, the STP will be calculate again and the port state will change. This is the basic theory of STP.

STP Disadvantage

With the development of network technology and intensive application, the disadvantage of STP in the application has also been exposed. The defect of STP is mainly manifested in the convergence rate.

When the topology changes, the new configuration message spreads to the whole network after a period of time. This time delay is called Forward Delay. The protocol default value is 15s. Before all bridges receive this changing message, there may be a temporary loop if the port in forwarding state of the old topology does not find itself to stop transmitting data in the new topology. In order to solve the temporary loop problem, STP uses a timer policy. That is to add an intermediate state for the port which just learns MAC address and does not participate in forwarding when the port is from the blocking state to the forwarding state. The time of two state switching is Forward Delay. This can guarantee that there is not temporary loop when topology changes. But this is seemingly good solution actually brings the convergence time at least two times Forward Delay. In some real-time services (such as voice and video) it is not acceptable.

8.2.2 RSTP Introduction

RSTP Advantage

In order to solve the convergence rate defect of STP, the IEEE defined RSTP based on IEEE 802.1w standard in 2001. There are three important improvements in RSTP based on STP. It quickens the convergence rate (in 1s at fastest).

- Configure the two roles of Alternate Port and Backup Port for the root port and designated port fast switching. When the root port is non-effective, the alternate port will fast switch to be the new root port and go into the forwarding state without delay. When the designated port is non-effective, the backup port will fast switch to be the new designated port and go into the forwarding state without delay.
- In the point to point link only connecting two Switch interfaces, the designated interface only needs to shake hand with the downstream bridge once time and then can enter the forwarding state without any delay. If it is the sharing link connecting three bridges or above, the downstream bridge will not response to the handshake request sent out by the designated interface of upstream bridge and only can wait two times of Forward Delay time to enter the forwarding state.
- The interface directly connects with the terminal and does not connect with other bridges is defined to be the Edge Port. The edge port can go into the forwarding state directly without any delay. Because the bridge cannot know whether the port connecting with the terminal or not, it needs to be configured manually.

RSTP Disadvantage

The RSTP has many improvements compared with the STP and can be compatible with the STP downward and can be mixed network. But, RSTP belongs to the SST (Single Spanning Tree) as STP. It has so many disadvantages mainly displaying the following three aspects.

- Because the whole network has only one tree, the convergence time will be too long when the network size is large.
- Because the RSTP is single spanning tree protocol and all VLAN share one tree, every VLAN in the network must be continuously distributed along the tree path direction in order to ensure normal communication in VLAN. Otherwise, there will be some VLAN separated due to the internal link is blocked. This will cause the problem that bridges in VLAN cannot communicate with each other.

- When one link is blocked, it will not carry any flow and will be unable to achieve load balance. This causes enormous waste of bandwidth.

All these defects of single spanning tree cannot be overcome. So the MSTP supporting VLAN appears.

8.2.3 MSTP Introduction

MSTP Advantage

The MSTP is a new spanning tree protocol defined in IEEE 802.1s. Compared with the STP and RSTP, its advantage is very obvious. Its features are as the following.

- The MSTP introduces the concept of “domain” to divide one switching network into several domains. There are multiple trees in every domain. These spanning tress are independent of each other. Among these domains, the MSTP uses CIST to ensure that there is no loop existed in the network.
- The MSTP introduces the concept of “Instance” to map multiple VLAN into one instance. This can save communication cost and resource occupancy rate. Each instance topology calculation of the MSTP is independent (each instance corresponding to a single spanning tree). In these instances, VLAN data sharing can be loaded.
- The MSTP can achieve rapid migration mechanism of port state similar to the RSTP.
- The MSTP can be compatible with the STP and RSTP.

MSTP Algorithm

1. Initial State

   Each port of each device generates one configuration message that makes it to be the root bridge at the initial time. The total root and domain root are its bridge ID. The outer root path cost and inner root path cost are all zero. The designated bridge ID is this bridge ID itself. The designated port is the bridge port itself. The port receiving BPDU message is zero.

2. Interface Role Selection Principle

   The selection principle of port role is shown as the Table 8-1.

Table 8-1 Interface Role Selection Principle

Port Role	Choosing Principle
Root Interface	Port priority vector is better than the designated priority vector of the port. And the root priority vector of device derives from the root path priority vector of the port.
Designated Interface	The designated priority vector of port is better than the port priority vector.
Master Interface	The role of domain boundary root port in MSTI instance is the Master port.
Alternate Interface	Port priority is better than the designated priority vector of the port. But the root priority vector of device does not derive from the root path priority vector of the port.
Backup Interface	Port priority is better than the designated priority vector of the port. But the designated ID of port priority vector is the bridge ID of local device.

3. Priority Vector Calculation

The MSTP role of all bridges is computed according to the carrying information in the message. The most important information carried in the message is the priority vector of the spanning tree. We will introduce the CIST priority vector and MSTI priority vector calculation method as follow.

a) CIST Priority Vector Calculation

In CIST, priority vector is composed of the total root, outer root path cost, domain root, inner root path cost, designated bridge ID, designated port ID and the ID of port receiving BPDU message.

In order to facilitate the subsequent description, we make the following assumptions.

- In the initial condition, the information carried in the message sent out by the PB port of the bridge B is as follow. The total root is RB. The outer root path cost is ERCB. The domain root is RRB. The inner root path cost is IRCB. The designated bridge ID is B. The designated port is B. The designated port ID is PB. The ID of port receiving BPDU message is PB.
- The information carried in the message which is received by PB port of bridge B from the PD port of bridge D is as follow. The total root is RD. The

outer root path cost is ERCD. The domain root is RRD. The inner root path cost is IRCD. The designated bridge ID is D. The designated port ID is PD. The ID of port receiving BPDU message is PB.

- The priority of message received by PB port of bridge B from PD port of bridge D is higher.

Based on the above assumptions, it will introduce the calculation method of the priority vector as follow.

(1) Message Priority Vector

The message priority vector is the priority vector carried in the MSTP protocol message. According to the assumption, The message priority vector received by the PB port of bridge B is { RD : ERCD : RRD : IRCD : D : PD : PB }.
If the bridge B and bridge D are not in the same domain, the inner root path cost is meaningless to bridge B and it will be set to be zero.

(2) Interface Priority Vector

In the initial condition, the port priority vector will make itself to be the root. The port priority vector of PB port is { RB : ERCB : RRB : IRCB : B : PB : PB }.

The port priority vector is updated according to the message priority vector received by port. If the message priority vector received by port is better than the port priority vector, then the port priority vector is updated to be the message priority vector. Otherwise, the port priority vector remains constant. Because the message priority vector received by PB port is better tha the port priority vector, the port priority is updated to be { RD : ERCD : RRD : IRCD : D : PD : PB }.

(3) Root Path Priority Vector

The root path priority vector is calculated by the port priority vector.

- If the port priority vector is from the bridge of different domain, the outer root path cost of the root path priority is the sum of the port path cost and the outer root path cost of port priority vector. The domain root of root path priority vector is the local bridge domain root. The inner root path cost is zero. Supposing that the PB port path cost of bridge B is PCPB, the root path

priority vector of PB port is { RD : ERCD+ PCPB : B : 0 : D : PD : PB }.

- If the port priority vector is from the bridge of the same domain, the inner path cost of the root path priority vector is the sum of the inner root path cost of the port priority vector and the port path cost. The root path priority vector of PB port after calculation is { RD : ERCD: RRD : IRCD + PCPB : D : PD : PB }.

(4) Bridge Priority Vector

The total root ID, domain root ID and designated bridge ID of bridge priority vector are all the local bridge ID. The outer root path cost and inner root path cost are all zero. The designated port ID and the receiving port ID are all zero. The bridge priority vector of bridge B is { B : 0 : B : 0 : B : 0 : 0 }.

(5) Root Priority Vector

The root priority vector is the better value between the bridge priority vector and the root path priority vector of all the designated bridge ID different with the local bridge ID. If the local bridge priority vector is better, then the local bridge is the CIST total root. Supposing that the bridge priority vector of bridge B is the best, then the root priority vector of bridge B is { B : 0 : B : 0 : B : 0 : 0 }.

(6) Designated Priority Vector

The designated priority vector of port is calculated from the root priority vector. The designated bridge ID of the root priority vector is replaced to be the local bridge ID and the designated port ID is replaced to be its own port ID. The designated priority vector of PB port of bridge B is { B : 0 : B : 0 : B : PB : 0 }.

b) MSTI Priority Vector Calculation

The calculation rule of each MSTI priority vector is basically the same as the CIST priority vector. There are two differences.

- There are not the total root and outer root path cost in MSTI priority vector. It is only composed of domain root, inner root path cost, designated bridge ID, designated port ID and the ID of port receiving BPDU message.
- MSTI only handles the message priority vector from the same domain.

4. Role Selection Process

The CIST instance calculation process will be introduced briefly as follow with the Figure 8-1. Supposing that the bridge priority of SwitchA is better than Switch B and the SwitchB is better than SwitchC. The link path costs are 4, 5 and 10. SwitchA and SwitchB belong to the same domain and SwitchC belongs to another domain alone.

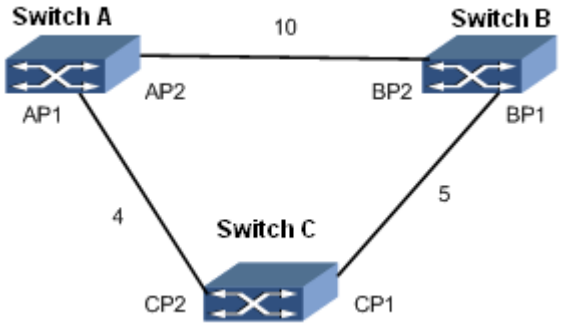


Figure MSTP Algorithm Calculation Process

The message priority vector carried in the message sent out by the device in initial state of the Figure 8-1 is shown in the Table 8-2.

Table 8-2 Initial State of Every Device

Device	**Port**	Message **Priority Vector**
Switch A	AP1	{A:0:A:0:A:AP1:0}
	AP2	{A:0:A:0:A:AP2:0}
Switch B	BP1	{B:0:B:0:B:BP1:0}
	BP2	{B:0:B:0:B:BP2:0}
Switch C	CP1	{C:0:C:0:C:CP2:0}
	CP2	{C:0:C:0:C:CP2:0}

The port priority vector of all ports of device keep the same as the message priority vector in initial state.

In initial state, the port of every device will be calculated to be the designated port and will send out the message priority vector which makes it to be the root Bridge.

a) Switch A Role Selection Process

The AP1 port and AP2 port of Switch A will receive the message from SwitchB and SwitchC respectively. SwitchA will compare the port priority vector of AP1 port and AP2 port with the message priority vector from other Switch. Because the port priority vector of port AP1 and AP2 are better than the message priority vector carried in the message, the role of port AP1 and AP2 does not change and is still the designated port and SwitchA is the total root and is the domain root of SwitchA and SwitchB. Since then, the port will send out the message which makes itself to be the root regularly.

b) Switch B Role Selection Process

After the BP1 port of SwitchB receiving the message from the CP1 port of SwitchC, it will compare the message priority vector with the port priority vector. Because the port priority vector is better than the message priority vector, the role of the port will not be updated.

After the BP2 port of SwitchB receiving the message from the AP2 port of SwitchA, the process is as follow.

(1) Compare the message priority vector of port with the port priority vector. Because the message priority of port is better than the port priority vector, the port priority vector will be updated to be the message priority vector {A:0:A:0:A:AP2:BP2};

(2) Calculate the root path priority vector of port. SwitchA and SwitchB are in the same domain. The port root path priority vector is {A:0:A:10:A:AP2:BP2};

(3) Calculate the root priority vector of SwitchB. Only the root path priority vector of BP2 port is from other device. Because the root path priority vector of BP2 port is better than the bridge priority vector of SwitchB, the root priority vector of SwitchB is {A:0:A:10:A:AP2:BP2};

(4) Specify the priority vector calculation. The designated priority vector of BP1 port is {A:0:A:10:B:BP1:BP2}. The designated priority vector of BP2 port is {A:0:A:10:B:BP2:BP2}.

Determine the role of the port: Compare the designated priority vector with the port priority vector of the BP1 port and BP2 port. Because the designated priority vector of BP1 is better than the port priority vector, the role of BP1 is the designated port and the BP1 port sends out the designated priority vector {A:0:A:10:B:BP1:BP2} which makes the SwitchA to be the total root and domain root regularly. Because the port

priority vector of BP2 is better than the designated priority vector and the root priority vector is from the root path priority vector of BP2 port, the role of BP2 is the root port.

c) Switch C Role Selection Process

The CP1 port of SwitchC receives the message priority vector {B:0:B:0:B:BP1:CP1} not updated of SwitchB. The CP2 port receives the message priority vector {A:0:A:0:A:AP1:CP2} from SwitchA. By comparing separately, the message priority vector of CP1 and CP2 are all better than the port priority vector. So the port priority vector of CP1 and the port priority vector of CP2 are separately updated to be {B:0:B:0:B:BP1:CP1} and {A:0:A:0:A:AP1:CP2}. Because SwitchC is not in the same domain with SwitchA and SwitchB, the root path priority vector of CP1 port is {B:5:C:0:B:BP1:CP1} and the root path priority vector of CP2 is {A:4:C:0:A:AP1:CP2}. The root path priority vector of CP2 is better than the root path priority vector of CP1, the root priority vector is {A:4:C:0:A:AP1:CP2}. The designated priority vector of CP1 and CP2 are separately the {A:4:C:0:C:CP1:CP2} and {A:4:C:0:C:CP2:CP2}. The CP1 port is calculated to be the designated port and the CP2 port is calculated to be the root port.

The CP1 port of SwitchC receives the updated message priority vector {A:0:A:10:B:BP1:CP1} from BP1. By comparing, the message priority vector of CP1 is better than its port priority vector and then it will update the port priority vector to be{A:0:A:10:B:BP1:CP1}. The calculated root path priority vector of CP1 port is {A:5:C:0:B:BP1:CP1}. Because the message priority vector received by CP2 port is not changed, according to the above calculation, the root path priority vector of CP2 port keeps to be {A:4:C:0:A:AP1:CP2}. The root path priority vector of CP2 is better than the root path priority vector of CP1, the root path priority vector is {A:4:C:0:A:AP1:CP2}. The designated priority vector of CP1 and CP2 port are {A:4:C:0:C:CP1:CP2} and {A:4:C:0:C:CP2:CP2} separately. The port priority vector of CP1 is better than its designated priority vector, but the root priority vector is not from the root path priority vector of CP1 port. Therefore the role of CP1 is Alternate Port. CP2 is still the root port.

5. Calculation Result

After the role of device and interface determines, the whole tree topology is established completely. The flow forwarding path is shown as the Figure 8-2 after the above calculation.

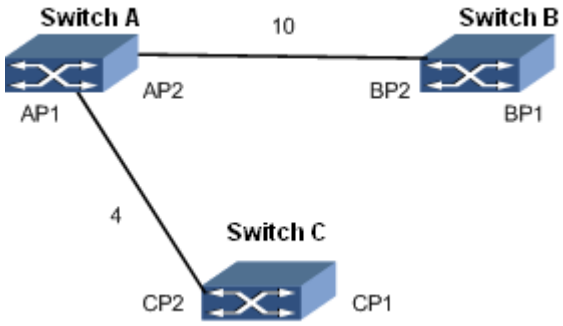


Figure Flow Forwarding Path after Calculation

8.2.4 Configure Device to Join Designated MST Domain

Background Information

As long as the same configuration, the two switches belong to the same domain.

- MST domain name
- MSTI and VLAN mapping relationship
- MST domain revision level

Before configuring Switch to join designated MST domain, it needs to configure physical attribute of interface and interface VLAN characteristic.

Purpose

This section introduces how to configure Switch to join MST domain.

Process

According to different destination, please execute corresponding steps. Refer to the following table.

Objective	Procedure
Configure STP working mode of Switch	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **stp** to enter STP Configuration View; 3. Use command of **stp mode** { **stp** | **rstp** | **mstp** | **default** } to configure STP working mode of Switch; 4. End.
Configure MST domain	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **stp** to enter STP Configuration View 3. Use command of **stp config-name** *string* to configure MST domain name;

Objective	Procedure
	4. Use command of **stp instance** *instance-id* **vlan** *vlan-list* to configure applied VLAN of MSTI; 5. Use command of **stp revision-level** { *range* | **default** } to configure MSTP revision level; 6. End.
Configure whether to enable interface STP function	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter Interface Configuration View; 3. Use command of **stp** { **enable** | **disable** } to enable or disable interface STP function; 4. End.
(Optional) Configure priority of Switch in designated MSTI	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **stp** to enter STP Configuration View 3. Use command of **stp instance** *instance-id* **priority** { *priority* | **default** } to configure priority of Switch in designated MSTI; 4. End.
(Optional) Configure priority of CIST instance 0	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **stp** to enter STP Configuration View 3. Use command of **stp priority** { *priority* | **default** } to configure priority of CIST instance 0; 4. End.
(Optional) Configure interface priority	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter Interface Configuration View; 3. Use command of **stp priority** { *priority* | **default** } to configure interface priority; 4. End.

Attached List:

Parameter	Description	Value
string	STP domain name	Character string without blank
instance-id	STP instance ID	to be from 1 to 63
range	STP revision level	to be from 0 to 65535
priority	QSW-2870 priority, the value is smaller, the priority is higher	to be from 0 to 61440, step by 4096, can configure number of 16 priority, such as 0,4096, 8192 and etc.
customer	Bridge type to be customer mode	-
provider	Bridge type to be provider mode	-
priority	Interface priority	to be from 0 to 240

8.2.5 Configure MSTP Parameter

Background Information

Before modifying MSTP parameters, please first finish the following tasks.

- Configure interface physical attribute
- Configure interface to join in VLAN
- Configure Switch to join in designated MST domain

Purpose

Introduce how to modify MSTP parameters in this section.

In some specific network environment, user can modify MSTP parameters to achieve the best result.

Process

According to different destination, please execute corresponding steps. Refer to the following table.

Objective	Procedure
Configure STP forward delay	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **stp** to enter STP Configuration View 3. Use command of **stp forward-delay** { *forward-delay* | **default** } to configure STP forward delay; 4. End.
Configure interval to send hello message for protocol	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **stp** to enter STP Configuration View 3. Use command of **stp hello-time** { *hello-interval* | **default** } to configure interval to send hello message for protocol; 4. End.
Configure the maximum aging time of Switch STP	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **stp** to enter STP Configuration View 3. Use command of **stp max-age** { *max-age* | **default** } to configure the maximum aging time of Switch STP; 4. End.
Configure the maximum hops of STP MST domain	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **stp** to enter STP Configuration View 3. Use command of **stp max-hop** { *max-hop* | **default** } to configure the maximum hops of STP MST domain; 4. End.

Objective	Procedure
Configure whether to be edge port	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter Interface Configuration View; 3. Use command of **stp** { **enable** | **disable** } to enable or disable interface STP function; 4. Use command of **stp edge-port** { **enable** | **disable** } to enable or disable interface to be edge port; 5. End.
Configure interface whether to be point to point management	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter Interface Configuration View; 3. Use command of **stp** { **enable** | **disable** } to enable or disable interface STP function; 4. Use command of **stp point-to-point** { **true** | **false** } to configure interface link type; 5. End.
Configure current interface priority of designated MSTI	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter Interface Configuration View; 3. Use command of **stp** { **enable** | **disable** } to enable or disable interface STP function; 4. Use command of **stp instance** *instance-id* **priority** { *priority* | **default** } to configure current interface priority of designated MSTI; 5. End.
Configure current interface management path cost of designated MSTI	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter Interface Configuration View; 3. Use command of **stp** { **enable** | **disable** } to enable or disable interface STP function; 4. Use command of **stp instance** *instance-id* **path-cost** { *path-cost* | **default** } to configure current interface management path cost of designated MSTI; 5. End.
Configure seding packet times during Hello Time interval of STP(sending BPDU number)	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **stp** to enter STP Configuration View 3. Use command of **stp transmit-limit** { *transmit-limit* | **default** } to Configure seding packet times during Hello Time interval of STP ; 4. End.
Configure interface	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* or

Objective	Procedure
management path cost of instance 0	**interface eth-trunk** *trunk-number* to enter Interface Configuration View; 3. Use command of**stp** { **enable** | **disable** } to enable or disable interface STP function; 4. Use command of**stp path-cost** { *cost* | **default** } to configure interface management path cost of instance 0; 5. End.
Configure count standard of STP interface path cost	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **stp** to enter STP Configuration View 3. Use command of **stp pathcost-standard** { **dot1t** | **dot1d-1998** } to configure count standard of STP interface path cost; 4. End.
Configure current interface to execute mode check operation	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter Interface Configuration View; 3. Use command of **stp** { **enable** | **disable** } to enable or disable interface STP function; 4. Use command of**stp mcheck** to configure current interface to execute mode check operation 5. End.
Configure STP migration time cycle	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **stp** to enter STP Configuration View 3. Use command of **stp migration-time** { *migration-time* | **default** } to configure STP migration time cycle; 4. End.
Configure whether to enable point-to-point link detection	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **stp** to enter STP Configuration View 3. Use command of **stp link-detection** { **enable** | **disable** } to enable or disable point-to point link detection; 4. End.
Configure whether to enable STP Trap function	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **stp** to enter STP Configuration View 3. Use command of **stp trap** { **enable** | **disable** } to enable or disable STP Trap function; 4. End.

Attached List:

Parameter	Description	Value
forward-delay	STP forward delay	to be from 4 to 30, unit: second
default	Default value	15s

Parameter	Description	Value
hello-interval	STP hello message interval	to be from 1 to 10, unit: second
default	Default interval	2s
max-age	STP max aging time	to be from 6 to 40, unit: second
default	Default max aging time	20s
max-hop	STP max hop	to be from 4 to 30, unit: hop
default	Default max hop	20hops
instance-id	STP instance ID	to be from 1 to 63
priority	Interface priority	to be from 0 to 240, step by 16
default	Default value	128
path-cost	Port cost	to be from 0 to 200000
default	Default value	0
transmit-limit	Times of sending hello packet	to be from 1 to 255, unit: times
default	Default value	3times
cost	Interface path cost	to be from 0 to 200000
default	Default value	0
{ dot1t | dot1d-1998 }	dot1t means IEEE 802.1t standard, dot1d-1998 means IEEE 802.1D standard	-
migration-time	STP protocol migration time	to be from 1 to 10, unit: second
default	Default value	3s
interface-number	Ethernet interface number	to be from <1-12>/<1-18>
trunk-number	Trunk interface number	to be from 1 to 128

8.2.6 Configure MSTP Protection Function

Background Information

- BPDU protection

  For the access layer device, the access interface usually connects with user terminal (such as PC) or file server. At this time, the access interface can be configured the as edge interface to realize interface fast switching. Under normal circumstances, the edge interface will not receive BPDU message of STP. But if anyone forges configuration message and attacks switch maliciously. When the edge interface receives the configuration message, system will configure these interfaces to be non-edge interface automatically and will calculate STP again. This will results in network topology concussion. BPDU protection function can prevent this network attack.

- Loop protection

  The root port and other blocked ports state maintains by receiving BPDU from upstream Switch continuously. When it causes that these ports cannot receive BPDU from upstream Switch because of link congestion or link failure, Switch will select the root port over again. The original root port will change to the designated port and the original blocked port will migrate to the forwarding state. This will lead to loop of switching network.

  Loop protection function will inhibit loop. After enabling loop protection function, if the root port cannot receive BPDU from upstream, it will be configured to be blocked state. And the blocked port will maintain blocked state and not forward message so there will not be any loop in the network.

- Root protection

  The root protection function can be used to prevent the unknown source or origin BPDU from changing network topology.

  Due to the mistaken configuration of maintainer or malicious network attack, the legal root bridge may receive configuration message with higher priority in the network. So the current root bridge will lose the root bridge position and lead to error change of network topology. Assuming that the original flow is forwarded through the high-rate link, the illegal change will cause that the flow of high-rate link is pulled into low-rate link and make network congestion. Root protection function can prevent this condition from happening.

  For these ports configured root protection function, the role of port only maintains to be designated port. Once this kind of ports receive configuration message with higher priority, the state of these ports will be configured as listening state and not forward message (equivalent to the link which the port connected disconnecting). During long enough time, if not receiving better configuration message, the port will restore the original state.

- TC protection

  After Switch receiving TC-BPDU message, it will delete MAC table item and ARP table item. If someone forges TC-BPDU packet to attack Switch maliciously, the Switch will receive a lot of TC-BPDU messages in a short time. And frequent

deletion operation will cause great burden to the device and bring great hidden trouble to the network stability.

After enabling TC-BPDU message attack function, the number of times which MSTP processes BPDU message of TC type can be configured per unit time. If the number of BPDU messages of TC type received by MSTP process exceeds the configured threshold, the MSTP process only deals with the designated times specified by threshold. For other BPDU messages of TC type beyond the threshold, after the timer expires, MSTP process only deals with once. In this way, it can avoid frequent deletion of MAC table item and ARP table item so as to protect the Switch.

Purpose

When need to configure MSTP protection, user can use this section operation.

Process

According to different destination, please execute corresponding steps. Refer to the following table.

Objective	Procedure
Configure BPDU protection function	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **stp** to enter STP Configuration View 3. Use command of **stp bpdu-guard** { **enable** | **disable** } to configure BPDU protection function; 4. End.
Open BPDU protection blocked port	1. Use command of **configure** to enter Global Configuration View; 2.Use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter Interface Configuration View; 3. Use command of **stp bpdu-guard-forward** to open BPDU protection blocked port; 4. End.
Configure Switch loop protection function	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **stp** to enter STP Configuration View 3. Use command of **stp loop-protection** { **enable** | **disable** } to configure Switch loop protection function; 4. End.

Objective	Procedure
Configure Switch root protection function	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **stp** to enter STP Configuration View 3. Use command of **stp root-protection** { **enable** | **disable** } to configure Switch root protection function; 4. End.
Configure root protection function of designated MSTI	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **stp** to access STP configuration view; 3. Use command of **stp instance** *instance-id* **root-protection** { **enable** | **disable** } to configure root protection function of designated MSTI; 4. End.
Configure Switch TC protection function	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **stp** to enter STP Configuration View 3. Use command of **stp tc-protection** { **enable** | **disable** } to configure Switch TC protection function; 4. Use command of **stp tc-hold-off** { *time* | **default** } to configure topology to change delay/restrain time; 5. End.

Attached List:

Parameter	Description	Value
time	delay/restrain time	To be from 4 to 30, unit: second
default	default value	10s
instance-id	STP instance ID	To be from 1 to 63

8.2.7 Maintenance and Debug

Purpose

When MSTP function is abnormal, user can use this operation to check or debug.

Process

According to different destination, please execute corresponding steps. Refer to the following table.

Objective	Procedure
Enable STP	1. Keep current Privileged User View;

Objective	Procedure
debug function	2. Use command of **debug stp** { **error** | **statemachine** | **timer** | **in** | **out** | **packet** | **protocol** | **event** | **all** } to enable STP debug function; 3. End.
Disable STP debug function	1. Keep current Privileged User View; 2. Use command of **no debug stp** { **error** | **statemachine** | **timer** | **in** | **out** | **packet** | **protocol** | **event** | **all** } to disable STP debug function; 3. End.
Check configuration information of Switch STP	1. Use command of **disable** to exit to Normal User View, or use command of **configure** to enter Global Configuration View, or use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter Interface Configuration View, or use command of **stp** to enter STP Configuration View or no use any command to keep current Privileged User View; 2. Use command of **show stp** to display configuration information of Switch STP; 3. End.
Check configuration file information of Switch STP	1. Use command of **disable** to exit to Normal User View, or use command of **configure** to enter Global Configuration View, or use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter Interface Configuration View, or use command of **stp** to enter STP Configuration View or no use any command to keep current Privileged User View; 2. Use command of **show stp config** to display configuration file information of Switch STP; 3. End.
Check related information of Switch STP	1. Use command of **disable** to exit to Normal User View, or use command of **configure** to enter Global Configuration View, or use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter Interface Configuration View, or use command of **stp** to enter STP Configuration View or no use any command to keep current Privileged User View; 2. Use command of **show stp information** to display related information of Switch STP; 3. End.
Check STP instance configuration information of all interface or designated	1. Use command of **disable** to exit to Normal User View, or use command of **configure** to enter Global Configuration View, or use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter Interface Configuration View, or use command of **stp** to enter STP Configuration View or no use any command to keep current Privileged User View;

Objective	Procedure
interface	2. Use command of **show stp instance** *instance-id* **interface** to display STP instance configuration information of all interface ; Or Use command of **show stp instance** *instance-id* **interface** fastethernet *interface-number* to display STP instance configuration information of designated interface ; 3. End.
Check configuration information of all interface STP	1. Use command of **disable** to exit to Normal User View, or use command of **configure** to enter Global Configuration View, or use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter Interface Configuration View, or use command of **stp** to enter STP Configuration View or no use any command to keep current Privileged User View; 2. Use command of **show stp interface** to display configuration information of all interface STP; 3. End.
Check configuration information of designated interface STP	1. Use command of **disable** to exit to Normal User View, or use command of **configure** to enter Global Configuration View, or use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter Interface Configuration View, or use command of **stp** to enter STP Configuration View or no use any command to keep current Privileged User View; 2. Use command of **show stp interface** fastethernet *interface-number* Or Use command of **show stp interface eth-trunk** *trunk-number* to display configuration information of designated interface STP; 3. End.

Attached List:

Parameter	Description	Value
interface-number	Ethernet interface number	to be from <1-12>/<1-18>
trunk-number	Trunk interface number	to be from 1 to 128
instance-id	MSTI ID	to be from 1 to 63

8.2.8 Example

Network Requirements

Now there are four Switches to support MSTP protocol. They are SwitchA, SwitchB, SwitchC and SwitchD. SwitchA and SwitchB are the QSW-2870 series Switch. SwitchC and SwitchD are other series Switch produced by Qtech. Configure MSTP basic function as following:

- SwitchA and SwitchC are in the same domain, domain name is Domain1 and craeate instance 1.
- SwitchB and SwitchD are in another same domain, domain name is Domain2 and create instance 1.
- SwitchA is CIST root.
- In Domain1, SwitchA is CIST domain root and instance 1 domain root. Configure root protection on interface of fe1/1 and fe1/2 of SwitchA.
- In Domain2, SwitchB is CIST domain root and SwitchD is instance 1 domain root.
- FE1/1 of SwitchC and SwitchD are configured as edge port and enable BPDU protection function at the same time.

Network Diagram

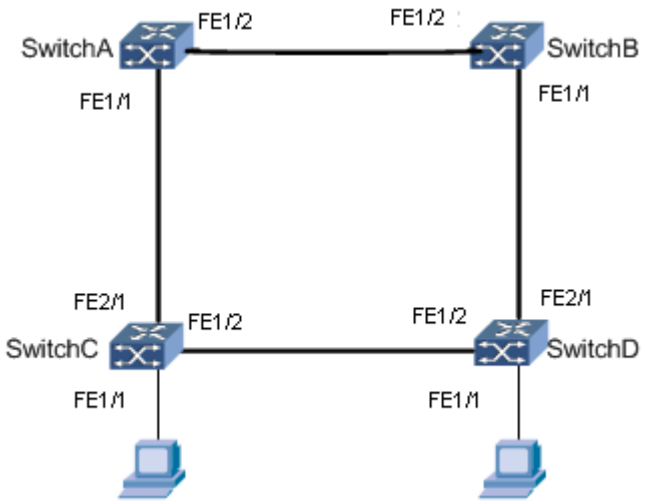


Figure MSTP Topology

Configuration Steps

1. Configure SwitchA.

//Configure SwitchA to join in Domain1.

```
SwitchA#configure
  %Enter configuration commands.End with Ctrl+Z or command "quit" & "end"
SwitchA(config)#stp
SwitchA(config-stp)#stp mode mstp
```

SwitchA(config-stp)#stp config-name Domain1

SwitchA(config-stp)#stp instance 1 vlan 1-10

SwitchA(config-stp)#stp revision-level 1

//Configure priority to be 0 of SwitchA in instance 0 to guarantee SwitchA to be as the CIST root.

SwitchA(config-stp)#stp priority 0

//Configure priority to be 0 of SwitchA in instance 1 to guarantee SwitchA to be as domain root of instance 1.

SwitchA(config-stp)#stp instance 1 priority 0

//Create VLAN2~VLAN 20 and add interface fe1/1 and fe1/2 of SwitchA to VLAN1~VLAN20, enable interface STP function and enable interface root protection function.

SwitchA(config)#vlan 2-20

SwitchA(config)#interface fastethernet1/1

SwitchA(config-fe1/1)#port link-type trunk

SwitchA(config-fe1/1)#port trunk allow-pass vlan 1-20

SwitchA(config-fe1/1)#stp enable

SwitchA(config-fe1/1)#quit

SwitchA(config)#stp

SwitchA(config-stp)#stp instance 1 root-protection enable

SwitchA(config-stp)#stp root-protection enable

SwitchA(config)#interface fastethernet1/2

SwitchA(config-fe1/2)#port link-type trunk

SwitchA(config-fe1/2)#port trunk allow-pass vlan 1-20

SwitchA(config-fe1/2)#stp enable

SwitchA(config-fe1/2)#quit

SwitchA(config)#stp

SwitchA(config-stp)#stp instance 1 root-protection enable

SwitchA(config-stp)#stp root-protection enable

SwitchA(config-stp)#

2. Configure SwitchB.

//Add SwitchB to Domain2.

SwitchB#configure

%Enter configuration commands.End with Ctrl+Z or command "quit" & "end"

SwitchB(config)#stp

SwitchB(config-stp)#stp mode mstp

SwitchB(config-stp)#stp config-name Domain2

SwitchB(config-stp)#stp instance 1 vlan 1-10

SwitchB(config-stp)#stp revision-level 2

//Configure priority to be 4096 of SwitchB in instance0 to guarantee SwitchB to be as CIST root.

SwitchB(config-stp)#stp priority 4096

//Create VLAN2~VLAN20 and add fe1/1 and fe1/2 of SwitchB to VLAN1~VLAN20, enable interface STP function, enable interface root protection function.

SwitchB(config)#vlan 2-20

SwitchB(config)#interface fastethernet1/1

SwitchB(config-fe1/1)#port link-type trunk

SwitchB(config-fe1/1)#port trunk allow-pass vlan 1-20

SwitchB(config-fe1/1)#stp enable

SwitchB(config-fe1/1)#quit

SwitchB(config)#interface fastethernet1/2

SwitchB(config-fe1/2)#port link-type trunk

SwitchB(config-fe1/2)#port trunk allow-pass vlan 1-20

SwitchB(config-fe1/2)#stp enable

SwitchB(config-fe1/2)#quit

SwitchB(config)#

3. Configure SwitchC.

//Add SwitchC to Domain1.

SwitchC#configure

%Enter configuration commands.End with Ctrl+Z or command "quit" & "end"

SwitchC(config)#stp

SwitchC(config-stp)#stp mode mstp

SwitchC(config-stp)#stp config-name Domain1

SwitchC(config-stp)#stp instance 1 vlan 1-10

SwitchC(config-stp)#stp revision-level 1

//Enable BPDU protection function.

SwitchC(config-stp)#stp bpdu-gurad enable

//Create VLAN2~VLAN20, add fe1/2 and fe2/1 of SwitchC to VLAN1~VLAN20, enable interface STP function, configure fe1/1 to be edge port.

SwitchC(config)#vlan 2-20

SwitchC(config)#interface fastethernet2/1

SwitchC(config-fe2/1)#port link-type trunk

SwitchC(config-fe2/1)#port trunk allow-pass vlan 1-20

SwitchC(config-fe2/1)#stp enable

SwitchC(config-fe2/1)#quit

SwitchC(config)#interface fastethernet1/2

SwitchC(config-fe1/2)#port link-type trunk

SwitchC(config-fe1/2)#port trunk allow-pass vlan 1-20

SwitchC(config-fe1/2)#stp enable

SwitchC(config-fe1/2)#quit

SwitchC(config)#interface fastethernet1/1

SwitchC(config-fe1/1)#stp enable

SwitchC(config-fe1/1)#edged-port enable

SwitchC(config-fe1/1)#port hybrid pvid 20

SwitchC(config-fe1/1)#port hybrid vlan 20 untagged

SwitchC(config-fe1/1)#quit

SwitchC(config)#

4. Configure SwitchD.

//Add SwitchD to Domain2.

SwitchD#configure

%Enter configuration commands.End with Ctrl+Z or command "quit" & "end"

SwitchD(config)#stp

SwitchD(config-stp)#stp mode mstp

SwitchD(config-stp)#stp config-name Domain2

SwitchD(config-stp)#stp instance 1 vlan 1-10

SwitchD(config-stp)#stp revision-level 2

//Configure priority to be 0 of SwitchD in instance 1 to guarantee SwitchD to be as domain root of instance 1.

SwitchD(config-stp)#stp instance 1 priority 0

//Enable BPDU protection function.

SwitchD(config-stp)#stp bpdu-gurad enable

//Create VLAN2~VLAN20, add fe1/2 and fe2/1 of SwitchD to VLAN1~VLAN20, enable interface STP function, configure fe1/1 to be edge port.

SwitchD(config)#vlan 2-20

SwitchD(config)#interface fastethernet2/1

SwitchD(config-fe2/1)#port link-type trunk

SwitchD(config-fe2/1)#port trunk allow-pass vlan 1-20

```
SwitchD(config-fe2/1)#stp enable
SwitchD(config-fe2/1)#quit
SwitchD(config)#interface fastethernet1/2
SwitchD(config-fe1/2)#port link-type trunk
SwitchD(config-fe1/2)#port trunk allow-pass vlan 1-20
SwitchD(config-fe1/2)#stp enable
SwitchD(config-fe1/2)#quit
SwitchC(config)#interface fastethernet1/1
SwitchC(config-fe1/1)#stp enable
SwitchC(config-fe1/1)#edged-port enable
SwitchC(config-fe1/1)#port hybrid pvid 10
SwitchC(config-fe1/1)#port hybrid vlan 10 untagged
SwitchC(config-fe1/1)#quit
SwitchC(config)#
```

8.3 RLINK Configuration

8.3.1 RLINK Introduction

RLINK Background

Double uplink network is used to provide link backup. Usually use STP to block redundancy link to eliminate loop so as to avoid broadcast storm. But its performance cannot meet user"s need and is not suitable for the network environment of high requirement for convergence time. For the above reason, we propose RLINK solution.

Resilient Link

RLINK is resilient link. The solution is specially designed for double uplink network to realize main-standby redundancy backup and fast switching.

Monitor Link

MLINK is monitor link. It is an interface linkage solution for RLINK. It makes RLINK work under more safe and steady environment.

RLINK uses MLINK function to monitor uplink in order to achieve the purpose of uplink and downlink synchronization. After uplink is fault, Monitor Link group will shut down downlink automatically. After uplink recovers, downlink will also recover.

RLINK Characteristic supported of QSW-2870

- Link redundancy

  It provides redundancy and backup function of link for double uplink network environment. RLINK realizes that one uplink is transmitting and the other is blocked in order to prevent loop broadcast storm.

- Fast switching

  After the main link is fault, flow will switch to backup link fast in millisecond to guarantee normal data transmitting and to avoid data loss.

- Flexible networking

  RLINK protocol provides single point uplink mode and double points uplink mode. User can choose which mode to use according to application scene.

- Load sharing

  RLINK protocol realizes load sharing by separate flow protection based on VLAN. Different VLAN flow transmits along different paths.

- Uplink monitoring

  MLINK linkage function of RLINK is used to monitor uplink change to synchronize downlink state to reduce flow loss.

- Simple configuration and low cost

  This solution is designed for double uplink network to guarantee performance and simple configuration.

8.3.2 Configure Resilient Link Group Function

Background Information

When user is using RLINK, please guarantee that interface configured RLINK is not enabled MSTP. If interface is enabled STP, G8031, G8032, RER, ALB, ESR and etc, the interface cannot be enabled RLINK.

The two uplinks must use BFD or MLINK to monitor the whole link, or it makes the master and slave interface not to find the real fault link. If this condition happens, it will result loop problem because master and slave interface are both transmitted state after links recovering.

When RLINK group is RLINK activated state, RLINK group mode cannot be modified.

Purpose

Using the operation in this section to configure Resilient Link group and its basic function to realize redundancy link backup and fast switching under double uplinks network environment.

Process

According to different destination, please execute corresponding steps. Refer to the following table.

Objective	Procedure
Create RLINK group and enter its configuration view	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **rlink group** *rlink-group-number* to create RLINK group and enter its configuration view; If RLINK group has existed already, use this command to enter its configuration view directly; 3. End.
Configure RLINK group mode to be single or double mode	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **rlink group** *rlink-group-number* to enter RLINK Configuration View; 3. Use command of **type** { **single** | **double** } to configure RLINK group mode; 4. End.
Configure master and slave interface of RLINK group	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* to enter Interface Configuration View; 3. Use command of **join rlink** *rlink-group-number* { **master** | **slave** | **sender** } to add interface to RLINK group and designate this interface to be master or slave or sender; 4. End.
(Optional) Configure sending VLAN ID of RLINK protocol packet	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* to enter Interface Configuration View; 3. Use command of **rlink group** *rlink-group-number* **send-vlan** *vlan-id* to configure sending VLAN ID of RLINK protocol packet ; 4. End.
Configure protection VLAN of RLINK instance	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **rlink group** *rlink-group-number* to enter RLINK Configuration View; 3. Use command of **protect-vlan** *vlan-list* to configure protection VLAN of RLINK instance;

Objective	Procedure
	4. End.

Attached List:

Parameter	Description	Value
interface-number	Ethernet interface number	to be <1-12>/<1-18>
rlink-group-number	RLINK group number	to be from 1 to 16
master	Master interface	-
slave	Slave interface	-
sender	Sender interface	
group-list	Mirror group list ID	to be from 1 to 8, form as 1,3-5
vlan-list	Protection VLAN list	Form as 1,3,10-20 to be from 1 to 4094
vlan-id	VLAN ID of protocol packet	to be from 1 to 4094

8.3.3 Configure Monitor Link Group Function

Background Information

 Attention:

Rules to configure MLink group:

- One interface can be uplink interface of multiple MLINK groups.
- One interface can only be downlink interface of one MLINK group.
- One interface cannot be the uplink interface and downlink interface at the same time.
- Interface which has joined in eth-trunk cannot join in MLINK group.

Purpose

To use the operation in this section to configure Monitor Link group and its basic function to realize interface linkage function.

Process

According to different destination, please execute corresponding steps. Refer to the following table.

Objective	Procedure
Create MLINK group and enter its configuration view	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **mlink group** *mlink-group-number* to create MLINK group and enter its configuration view; If MLINK group has existed already, use this

Objective	Procedure
	command to enter its configuration view directly; 3. End.
Configure uplink and downlink interface of MLINK group	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* to enter Interface Configuration View; 3. Use command of **join mlink** *mlink-group-number* **role** { **uplink** | **downlink** } to add interface to MLINK group and designate the link of interface to be uplink or downlink; 4. End.
Configure interface whether to enable MLINK linkage function	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **interface fastethernet** *interface-number* to enter Interface Configuration View; 3. Use command of **mlink** { **enable** | **disable** } to enable or disable MLINK linkage function of interface; 4. End.

Attached List:

Parameter	Description	Value
mlink-group-number	MLINK group number	to be from 1 to 16
interface-number	Ethernet interface number	to be <1-12>/<1-18>
uplink	Uplink member interface of MLINK group	-
downlink	Downlink member interface of MLINK group	-

8.3.4 Configure RLINK Other Related Parameter

Background Information

When there is fault in the main link of RLINK group, it will switch to standby link. After the original main link fault recovers, in order to keep flow stability, the main link keeps blocked state and do not preempt. If needing to recover it to be the main link, user can use the following two methods.

- Enable RLINK returning function, after returning timer terminating, it will switch to the main link.
- Use manual main-standby switching of RLINK group to enforce link switching.

 Attention:

For link switching manually, according to different type of RLINK group, it is divided into single point mode manual switching and double point mode manual switching.

It needs the following requirements to realize main-standby switching.

- There are master and slave interface in Resilient Link group.
- It must allow to force switching for link state. The link state of master and slave links should be linkup. (Master is up and slave is down, if want to force master to be down and slave to be up, slave link must be linkup.)

Purpose

Use the operation in this section to configure other related parameters of RLINK. User can choose which step to use according to your need. But first RLINK group or MLINK group should be configured.

Process

According to different destination, please execute corresponding steps. Refer to the following table.

Objective	Procedure
Configure to main/backup link switching of RLINK group manually	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **rlink group** *rlink-group-number* to enter RLINK Configuration View; 3. Use command of **manual-change** to trigger link switching; 4. End.
Configure overtime multiple value of receiving the peer end protocol packet of RLINK group	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **rlink group** *rlink-group-number* to enter RLINK Configuration View; 3. Use command of **receive-timeout** *timeout-value* to configure overtime multiple value of receiving the peer end protocol packet of RLINK group ; 4. End.
Enable or disable RLINK returning function	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **rlink group** *rlink-group-number* to enter RLINK Configuration View; 3. Use command of **reverse** { **enable** | **disable** } to enable or disable RLINK returning function ; 4. End.
Configure returning time of RLINK group	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **rlink group** *rlink-group-number* to enter RLINK

Objective	Procedure
	Configuration View; 3. Use command of **reverse-time** *time-value* to configure returning time of RLINK group; 4. End.
Configure sending interval of protocol packet	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **rlink group** *rlink-group-number* to enter RLINK Configuration View; 3. Use command of **send-interval** *time-interval* to confiugre sending interval of protocol packet; 4. End.
Enable or disable RLINK or MLINK trap function	1. Use command of **configure** to enter Global Configuration View; 2. Use command of **rlink group** *rlink-group-numbe* to enter RLINK Configuration View or use command of **mlink group** *mlink-group-number* to enter MLINK Configuration View; 3. Use command of **trap** { **enable** | **disable** } to enalbe or disable RLINK or MLINK trap function; 4. End.

Attached List:

Parameter	Description	Value
timeout-value	Overtime multiple value of receiving the peer end protocol packet	to be from 10 to 50
time-value	Resilient Link returning time	to be from 3 to 60, unit:second
time-interval	Packet sending interval	to be from 50 to 10000, unit:millisecond

8.3.5 Maintenance and Debug

Purpose

When RLINK function is abnormal, user can use this operation to check or debug.

Process

According to different destination, please execute corresponding steps. Refer to the following table.

Objective	Procedure
Enable RLINK debug function	1. Use command of **disable** to exit to Normal User View, or use command of **configure** to enter Global Configuration View, or use command of **interface fastethernet** *interface-number* or **interface eth-trunk**

Objective	Procedure
	trunk-number to enter Interface Configuration View, or no use any command to keep current Privileged User View; 2. Use command of **debug rlink** { **receive** | **send** | **timer** | **linkchange** | **all** } to enable RLINK debug function; 3. End.
Disable RLINK debug function	1. Use command of **disable** to exit to Normal User View, or use command of **configure** to enter Global Configuration View, or use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter Interface Configuration View, or no use any command to keep current Privileged User View; 2. Use command of **no debug rlink** { **receive** | **send** | **timer** | **linkchange** | **all** } to disable RLINK debug function; 3. End.
Enable MLINK debug function	1. Use command of **disable** to exit to Normal User View, or no use any command to keep current Privileged User View; 2. Use command of **debug mlink** { **linkchange** | **all** } to enable MLINK debug function; 3. End.
Disable MLINK debug function	1. Use command of **disable** to exit to Normal User View, or no use any command to keep current Privileged User View; 2. Use command of **no debug mlink** { **linkchange** | **all** } to disable MLINK debug function; 3. End.
Check RLINK configuration file information	1. Use command of **disable** to exit to Normal User View, or use command of **configure** to enter Global Configuration View, or use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter Interface Configuration View, or no use any command to keep current Privileged User View; 2. Use command of **show rlink config** to display configuration file information of double uplinks redundancy function; 3. End.
Check information of all or designated RLINK group	1. Use command of **disable** to exit to Normal User View, or use command of **configure** to enter Global Configuration View, or use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter Interface Configuration View, or no use any command to keep current Privileged User View; 2. Use command of **show rlink group** [*rlink-group-number*] to display information of all or designated RLINK group; 3. End.
Check RLINK	1. Use command of **disable** to exit to Normal User View, or use command

Objective	Procedure
information of all or designated interface	of **configure** to enter Global Configuration View, or use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter Interface Configuration View, or no use any command to keep current Privileged User View; 2. Use command of **show rlink interface** or **show rlink interface** fastethernet *interface-number* to display RLINK information of all or designated interface 3. End.
Check MLINK configuration file information	1. Use command of **disable** to exit to Normal User View, or use command of **configure** to enter Global Configuration View, or use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter Interface Configuration View, or no use any command to keep current Privileged User View; 2. Use command of **show mlink config** to display configuration file information of uplink monitoring function; 3. End.
Check information of all or designated MLINK group	1. Use command of **disable** to exit to Normal User View, or use command of **configure** to enter Global Configuration View, or use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter Interface Configuration View, or no use any command to keep current Privileged User View; 2. Use command of **show mlink group** [*mlink-group-number*] to display information of all or designated MLINK group; 3. End.
Check MLINK information of all or designated interface	1. Use command of **disable** to exit to Normal User View, or use command of **configure** to enter Global Configuration View, or use command of **interface fastethernet** *interface-number* or **interface eth-trunk** *trunk-number* to enter Interface Configuration View, or no use any command to keep current Privileged User View; 2. Use command of **show mlink interface** or **show mlink interface** fastethernet *interface-number* to display MLINK information of all or designated interface; 3. End.

Attached List:

Parameter	Description	Value
receive	Packet received	-
send	Packet sent out	-
timer	timer	-

Parameter	Description	Value
link change	Link change	-
all	All information	-
interface-number	Ethernet interface number	to be1~12/1~48

8.3.6 Example

8.3.6.1 Configure Single Point Uplink

Network Requirements

In single point uplink network environment, configure RLINK function. The master and slave interfaces are on the same Switch. They are fe1/1 and fe1/2.

Network Diagram

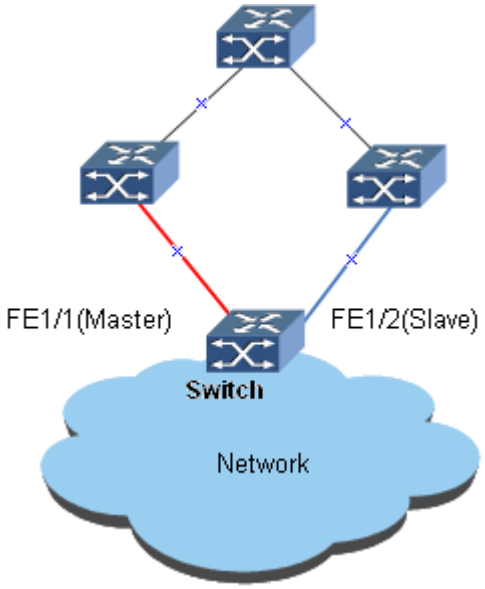


Figure Single Point Uplink Topology

Configuration Steps

1. Create RLINK group1.

Switch#configure

Switch(config)#rlink group 1

//Optional, default to be single mode

Switch(config-rlink1)#type single

//Configure protection VLAN. (RLINK group based on VLAN)

```
Switch(config-rlink1)#protect-vlan  1,2,3,4,5
//Activate RLINK group1
Switch(config-rlink1)#active
Switch(config-rlink1)#quit
Switch(config)#
```

2. Add fe1/1 to RLINK group1 and make it to be master interface.

```
Switch(config)#interface fastethernet 1/1
Switch(config-fe1/1)#join rlink group 1 master
Switch(config-fe1/1)#rlink enable
Switch(config-fe1/1)#quit
Switch(config)#
```

3. Add fe1/2 to RLINK group1 and make it to be slave interface.

```
Switch(config)#interface fastethernet 1/2
Switch(config-fe1/2)#join rlink group 1 slave
Switch(config-fe1/2)#rlink enable
Switch(config-fe1/2)#quit
Switch(config)#
```

4. Check RLINK group1 information.

```
Switch#show rlink group 1

Rlink group 1 information:
  Group status: active
  Group type: single
  Group vlanlist:
  Reverse: disable
  Reverse time: 0

  Member              Role     State      Status     Linkstate
  ge-1/1              MASTER   FORWARD    ACTIVE     up/up
  ge-1/2              SLAVE    BLOCK      ACTIVE     up/down
Switch#
```

8.3.6.2 Configure Double Points Uplink

Network Requirements

In double point‟s uplink network environment, configure RLINK function. Master interface and slave interface are configured separately on M1 and M2. The master interface is fe1/1 of M1 and slave interface is fe1/2 of M2.

Network Diagram

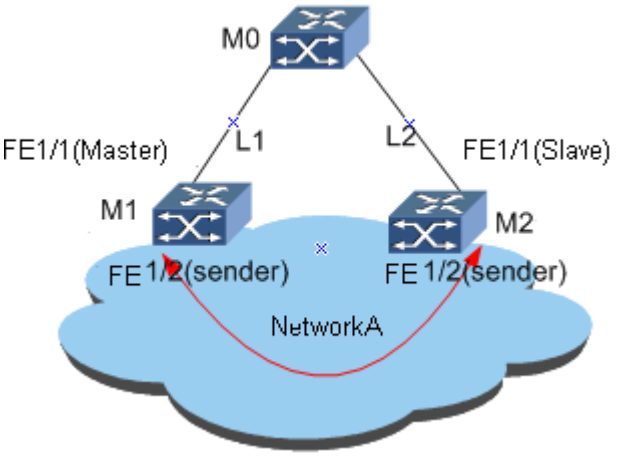


Figure Double Points Uplink Topology

Configuration Steps

1. Configure device M1.

//Create RLINK group1.

M1#configure

M1(config)#rlink group 1

M1(config-rlink1)#type double

M1(config-rlink1)#active

M1(config-rlink1)#quit

M1(config)#

//Add fe1/1 to RLINK group1 and make it to be master interface.

M1(config)#interface fastethernet 1/1

M1(config-fe1/1)#join rlink group 1 master

M1(config-fe1/1)#rlink enable

M1(config-fe1/1)#quit

M1(config)#

//Add fe1/2 to RLINK group1 and make it to be sender interface.

M1(config)#interface fastethernet 1/2

M1(config-fe1/2)#join rlink group 1 sender

M1(config-fe1/2)#rlink enable

M1(config-fe1/2)#quit

M1(config)#

2. Configure device M2.

//Create RLINK group1.

M2#configure

M2(config)#rlink group 1

M2(config-rlink1)#type double

M2(config-rlink1)#active

M2(config-rlink1)#quit

M2(config)#

//Add fe1/1 to RLINK group1 and make it to be master interface.

M2(config)#interface fastethernet 1/1

M2(config-fe1/1)#join rlink group 1 slave

M2(config-fe1/1)#rlink enable

M2(config-fe1/1)#quit

M2(config)#

//Add fe1/2 to RLINK group1 and make it to be sender interface.

M2(config)#interface fastethernet 1/2

M2(config-fe1/2)#join rlink group 1 sender

M2(config-fe1/2)#rlink enable

M2(config-fe1/2)#quit

M2(config)#

3. Check RLINK group1 information of M1.

M1#show rlink group

Rlink group 1 information:

Group status: active

Group type: double

Group vlanlist:

Reverse: disable

Reverse time: 0

Receive timeout: 15

Send interval: 2000

Peer exist: EXIST

Peer mac: 0:4:67:97:db:83

Peer role: SLAVE

Peer state: BLOCK

Peer Reverse: disable

Peer send interval: 2000

Peer linkstate: up

Member	Role	State	Sendvid	Status
ge-1/1	MASTER	FORWARD	0	ACTIVE
ge-1/2	SENDER	FORWARD	0	ACTIVE

8.3.6.3 Configure MLINK

Network Requirements

Configure MLINK on Switch, fe1/1 is uplink1, fe1/2 is uplink2, fe1/3 is downlink1, fe1/4 is downlink2.

Network Diagram

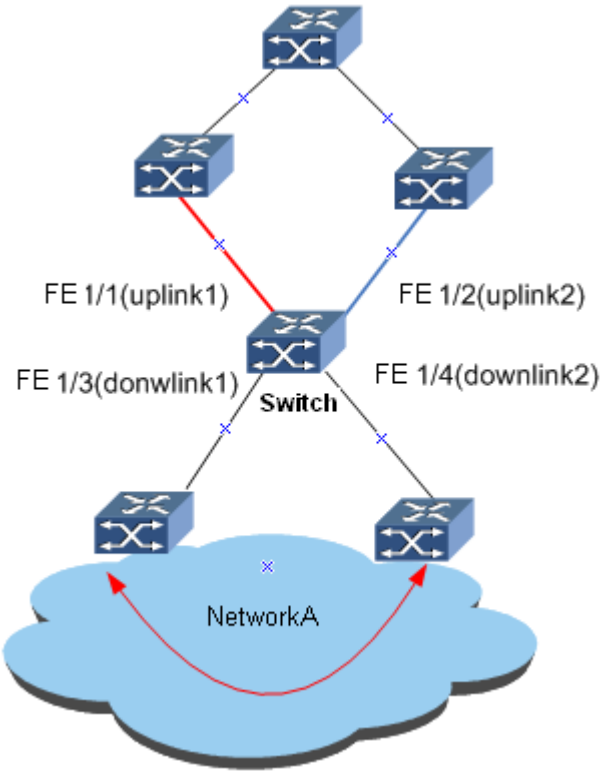


Figure MLINK Linkage Function Topology

Configuration Steps

1. Create MLINK group.

Switch#configure

Switch(config)#mlink group 1

Switch(config-mlink1)#quit

Switch(config)#

2. Add fe1/1 to MLINK group1 and make it to be uplink1 interface.

Switch(config)#interface fastethernet 1/1

Switch(config-fe1/1)#join mlink group 1 uplink

Switch(config-fe1/1)#mlink enable

Switch(config-fe1/1)#quit

Switch(config)#

3. Add fe1/2 to MLINK group1 and make it to be uplink2 interface.

Switch(config)#interface fastethernet 1/2

```
Switch(config-fe1/2)#join mlink group 1 uplink
Switch(config-fe1/2)#mlink enable
Switch(config-fe1/2)#quit
Switch(config)#
```

4. Add fe1/3 to MLINK group1 and make it to be downlink1 interface.

```
Switch(config)#interface fastethernet 1/3
Switch(config-fe1/3)#join mlink group 1 downlink
Switch(config-fe1/3)#mlink enable
Switch(config-fe1/3)#quit
Switch(config)#
```

5. Add fe1/4 to MLINK group1 and make it to be downlink2 interface.

```
Switch(config)#interface fastethernet 1/4
Switch(config-fe1/4)#join mlink group 1 downlink
Switch(config-fe1/4)#mlink enable
Switch(config-fe1/4)#quit
Switch(config)#
```

6. Check MLINK group configuration information.

```
Switch#show mlink group 1

Mlink group 1 information:
  Group status: active

  Member          Role       State      Status     Linkstate
  ge-1/1          UPLINK     FORWARD    ACTIVE     up/up
  ge-1/2          UPLINK     FORWARD    ACTIVE     up/up
  ge-1/3          DOWNLINK   FORWARD    ACTIVE     up/up
  ge-1/4          DOWNLINK   FORWARD    ACTIVE     up/up
Switch#
```

Chapter9
PoE Configuration

9.1 Summary

The full name of PoE is Power over Ethernet. PoE means to supply electricity by 10BASE-T, 100BASE-TX and 1000BASE-T Ethernet network. Its longest reliable power supply distance is 100 meters. In this way, it can effectively solve the problem of centralized power supply for the IP telephone, wireless AP, portable charger, credit card reader, camera, data acquisition terminal and etc. For these terminals, it does not need to consider the indoor power system wiring problems. It can realize the power supply for the equipment when they are in the access the network at the same time. In general use, the current power supply of PoE has the uniform standards. As long as we follow the released 802.3af or 802.3at standard, the different manufactures matching problem can be solved.

This chapter includes the following section.

9.2 PoE Function Configuration

9.2.1 Enable or Disable PoE Power Supply Function

Purpose

User can enable or disable remote power supply function of interface according to the network requirement by using the twisted pair for the external PD (Powered Device, electrical equipment). It provides more possibility for the application of the Ethernet at the access side.

Progress

According to the different purposes, execute corresponding step. Please refer to the following table.

Purpose	Step	Parameter
Enable power supply function of device Ethernet interface	1. Use command of **configure** 2. Use command of **interface fastethernet** interface-number or use command of **interface fastethernet** interface-number **to fastethernet** interface-number 3. Use command of **pse enable**	interface-number : interface number, integer, <1-12>/<1-18> enable: make the remote power supply function of device effective disable : make the remote power supply function of device non-effective
Disable power supply function of device Ethernet interface	1. Use command of **configure** 2. Use command of **interface fastethernet** interface-number or use command of **interface fastethernet** interface-number **to fastethernet** interface-number 3. Use command of **pse disable**	

9.2.2 Configure Power Supply mode

Background Information

QSW-2870-PE-PE supports four power supply modes. They are auto, force-standard, force-high and half-auto.

Generally, it is recommended that user uses the default mode of half-auto.

When the device cannot supply electricity normally using non-standard PD in half-auto mode, it is recommended that user uses the force-standard or force-high mode. If using one of the two modes, user must enable the enhanced detection power supply function.

Progress

According to the different purposes, execute corresponding step. Please refer to the following table.

Purpose	Step	Parameter
Configure interface power supply mode of device	1. Use command of **configure** 2. Use command of **interface fastethernet** interface-number or use command of **interface fastethernet** interface-number **to fastethernet** interface-number 3. Use command of **pse power-Management** { **auto** | **force-standard** | **force-high** | **half-auto** }	interface-number : interface number, integer, <1-12>/<1-18> auto: automatic mode of power supply force-standard: forced standard
(Optional)Ena	1. Use command of configure	

Purpose	Step	Parameter
ble the enchanced detection function of interface power supply	2. Use command of **interface fastethernet** interface-number or use command of **interface fastethernet** interface-number **to fastethernet** interface-number 3. Use command of **pse enhance-detect enable**	mode of power supply force-high: forced high power mode half-auto: half automatic mode enable: make enhanced detection power supply function effective

9.2.3 Configure PoE Power Supply Parameter

Background Information

Currently, QSW-2870-PE-PE only supports power supply in signal line mode, timing power supply and power supply alarm function.

Configure the PD device description connected with the interface on the device. It is convenient for user to manage the downstream PD device.

The PD device according with the 802.af protocol is the standard PD device. Usually, PSE can only detect the standard PD and supply electricity for it. After enabling PSE to detect the non-standard PD, PSE can detect the non-standard PD and supply electricity for it.

PoE power supply port supports three priorities. The port priority ensures that the critical equipment can be first powered when the power consumption of PD equipment is greater than the total power supplied by the PSE. When the PSE power is insufficient, if the priority of different ports is the same, it will order the priority according to the interface number. The interface number is greater the priority is higher and the port with greater interface number will be powered first.

The command of configuring the threshold power of PSE in the global configuration view is used to protect the Switch to avoid the influence of the unstable power supply.

Progress

According to the different purposes, execute corresponding step. Please refer to the following table.

Purpose	Step	Parameter
(Optional) Configure the description information of the device to be powered	1. Use command of **configure** 2. Use command of **interface fastethernet** interface-number or use command of **interface fastethernet** interface-number **to fastethernet** interface-number 3. Use command of **pse description** description	interface-number : interface number, integer, <1-12>/<1-18> description: description information, character string, 1~64 characters enable: make non-standard PD function detection effective power-value: the maximum power ration of interface, integer, 1~30000, unit: milliwatt low : the low priority high : the high priority critical : the highest priority none : cancel to bind with the time-range table item enable : bind with the time-range table item, power in the time configured
(Optional) Enable to detect non-standard PD function	1. Use command of **configure** 2. Use command of **interface fastethernet** interface-number or use command of **interface fastethernet** interface-number **to fastethernet** interface-number 3. Use command of **pse legacy enable**	
(Optional) Configure the maximum rated power ratio	1. Use command of **configure** 2. Use command of **interface fastethernet** interface-number or use command of **interface fastethernet** interface-number **to fastethernet** interface-number 3. Use command of **pse max power** power-value	
(Optional) Configure the priority of device interface power supply	1. Use command of **configure** 2. Use command of **interface fastethernet** interface-number or use command of **interface fastethernet** interface-number **to fastethernet** interface-number 3. Use command of **pse power-priority** { **low** | **high** | **critical** }	
(Optional) Configure power shutdown time range of device interface	1. After the step1, please enter the Global Configuration View 2. Use command of **interface fastethernet** interface-number or use command of **interface fastethernet** interface-number **to fastethernet** interface-number 3. Use command of **pse shutdown time-range** timerange	
(Optional) Enable or disable the trap alarm function of PSE	1. Use command of **configure** 2. Use command of **pse snmp-trap** { **enable** | **disable** }	

Purpose	Step	Parameter
(Optional) Configure the threshold value of the power utilization ratio	1. Use command of **configure** 2. Use command of **pse usage-threshold** threshold	disable : not bind with the time-range table item, not power in the tiem configured threshold : threshold value of power utilization ratio, integer, 1~99 timerange : integer, 1-128

9.2.4 Check PoE Configuration Information

Purpose

This operation is mainly used to check the configured PoE function and its parameters right or wrong.

Progress

According to the different purposes, execute corresponding step. Please refer to the following table.

Purpose	Step	Parameter
Check the configuration of Switch being as the PSE	1. Start device, input username and password to enter the Privilege User View or use command of **disable** to exit to the Common User View 2. Use command of **show pse config**	interface-number : interface number, integfer, <1-12>/<1-18>
Check the information of Switch being as the PSE	1. Start device, input username and password to enter the Privilege User View or use command of **disable** to exit to the Common User View 2. Use command of **show pse information**	
Check power supply information of all interfaces or the detailed power supply information of designated interface	1. Start device, input username and password to enter the Privilege User View or use command of **disable** to exit to the Common User View 2. Use command of **show pse interface** or use command of **show pse interface fastethernet** interface-number	

Appendix A

Example of generating initial public key document via Secure CRT:

---- BEGIN SSH2 PUBLIC KEY ----

Comment: "[2048-bit dsa, lsh@mini, Fri Apr 09 2004 03:58:53]"

AAAAB3NzaC1kc3MAAAEBAITV5xIOZ6T3851hLnLMr0UQkniu54Ci9YrMptaPE1Wy
Rx50lpwEPSLR4u+SspOd+tUhlV1yiOXn9o+P+c2Y2UIroo9Bi2YYQZJJDUnYJL7Kw
J0MSohOu6r1CT2Jdxr8wG0HMVqgA9FX95NEMZ5XF0np1XNDR2THNtk1Ybo7/Y3/
mp9cgyLTbHGkq1ZNDiPsBYp47rz3yXY67NlqTtfCfoF7FV1h7/Z9kiE0rofHYiRqZg+FJ
qCFdD2CsfaBsOUg1et872zSCPq+pGRzsoGPB5Kdlgl+wFC/5EA9yKyhqCfB9eDX4
HG0GDnK11AkBcxWgQBsDfMDhdrboaY3f+cC6A0AAAAVALvrsgVrh/ZWrGSObc4/1
QRO7PirAAABAHQibIe/yUc2aGp7p/bnB9RPrX7VuGi1XcybzwymwRDh7e4e9cdkFY
va+6YXPTBQjwnOGxcVtYBiY4BP2aSPj7SPU+RaBjkbcMYqpIEr2eFIAhJKd/mevZUh
OgPZsoviIJtbXAJrmcYGrzoC7iSkiNiowhz2/Yoe8/2m480czQke9lvuhgbVJryACCYpvK
yHdA2AXmAdWNC03gFQCgbBjozpxVuvoS0U5bucBjZ8EuL+h27oI79jY0uG2UbHgjh
bCiyRnmeNzpC3zFrp3WjgQP7+L6DwJq5QrnmZmQtGNhmhEQpoY+V20UypzITDP
MoV3DMCnQ2Es5EjTyMRmEsM6F0AAAEAAh4n4qNKmwsBM1+fS42NVKkDJa+cS
CpMxGuNYp5Gmqaorjq9C7zLvVLezcG9FTS65HPtj1P8aE5a/vu4aa6DCJWiJKBc+U
sM8X5L8MUtb2T3c69mLZptfi7x7x5ySwXepEQMr9fkif5cCd1EB4XRQ9Wf+jH41wms
JLMYwMi4CmHmzIGcWVA+U35m6mULrM+eJmvoUW7yG7lKPQpIygUv6WOBeB6F
hexW73zcuEh6Xlw0NDKBepP92+32ODVzansRj7yx44H9kfbwPKmv5Pgfs8ZPpTN4
2PUXnIxK6HIucmB4pUigC4bNT6QZLHaqu8ujQI4A8qbsvibW3Bu/r3a46g==

---- END SSH2 PUBLIC KEY ----

Tips of modification:

1、Remove “---- BEGIN SSH2 PUBLIC KEY ----”;

2、Remove “---- END SSH2 PUBLIC KEY ----”;

3、If „DSA‟ was selected when generating key, then change the “Comment: "[2048-bit dsa, lsh@mini, Fri Apr 09 2004 03:58:53]"” into “dsa ”, note that there is a blank space behind the „dsa;

If „RSA‟ was selected when generating key, then change the “Comment: "[2048-bit dsa, lsh@mini, Fri Apr 09 2004 03:58:53]"” into “rsa ”, note that there is a blank space behind the “rsa”;

4、Remove all the rest „Enter‟s (i.e., line break) in each line and change it into a txt with only one line.