Preface

Objectives

This document describes features and configurations of the QSW-8200 series switch, including Ethernet, route, reliability, OAM, security, and QoS, and provides configuration examples.

The appendix lists terms, acronyms, and abbreviations involved in this document.

By reading this document, you can master principles and configurations of the QSW-8200 series switch, and how to network with the QSW-8200 series switch.

Conventions

Symbol conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
⚠ Warning	Indicate a hazard with a medium or low level of risk which, if not avoided, could result in minor or moderate injury.
⚠ Caution	Indicate a potentially hazardous situation that, if not avoided, could cause equipment damage, data loss, and performance degradation, or unexpected results.
✎ Note	Provide additional information to emphasize or supplement important points of the main text.
🔍 Tip	Indicate a tip that may help you solve a problem or save time.

General conventions

Convention	Description
Times New Roman	Normal paragraphs are in Times New Roman.

Convention	Description
Arial	Paragraphs in Warning, Caution, Notes, and Tip are in Arial.
Boldface	Names of files, directories, folders, and users are in **boldface**. For example, log in as user **root**.
Italic	Book titles are in *italics*.
`Lucida Console`	Terminal display is in `Lucida Console`.

Command conventions

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

Contents

Tables

1 Basic configurations

This chapter describes basic configuration and configuration process about the QSW-8200 series switch, and provides related configuration examples, including the following sections:

- Accessing device
- CLI
- Managing files
- Managing configuration files
- Time management
- Interface management
- Configuring basic information
- Configuring management and auxiliary interfaces
- Configuring task scheduling
- Watchdog
- Auto-loading
- Software upgrade
- Configuration examples

1.1 Accessing device

1.1.1 Introduction

The QSW-8200 series switch can be configured and managed in Command Line Interface (CLI) mode or NMS mode.

The QSW-8200 series switch CLI mode has a variety of CLI configuration modes:

- Console mode: you must use Console mode for the first time of configuration. The QSW-8200 series switch supports two types of Console interfaces: RJ45 and USB.
- Telnet mode: log on in Console mode, start the Telnet service on the QSW-8200 series switch, configure the IP address of the Layer 3 interface, user name, and password, and then you can start remote Telnet configuration.

- SSHv2 mode: before accessing the QSW-8200 series switch through SSHv2, you need to log in to the QSW-8200 series switch and start the SSHv2 service through the Console interface.

When configuring the QSW-8200 series switch in network management mode, you must configure the Layer 3 interface IP address through CLI first, and then configure the QSW-8200 series switch through the NMS.

Note

The configuration steps in this manual are in CLI mode.

1.1.2 Accessing through Console interface

The Console interface is an interface which is commonly used to connect the network device with a PC running terminal emulation programs. You can use this interface to configure and manage local devices. This management method can communicate directly without a network, so it is called out-of-band management. You can also perform configuration and management on the QSW-8200 series switch through the Console interface when the network fails.

In the following two conditions, you can only log in to the QSW-8200 series switch and configure it through the Console interface:

- The QSW-8200 series switch is powered on to start for the first time.
- Accessing the QSW-8200 series switch through Telnet fails.

The QSW-8200 series switch supports the RJ45 or USB Console interface. The RJ45 Console interface is marked "Console" while the USB Console interface is marked "USB".

Note

- The RJ45 Console interface and USB Console interface are mutually exclusive, and cannot be used concurrently.
- Use the CBL-RS232-DB9F/RJ45-2m/RoHS cable delivered with the QSW-8200 series switch when accessing through the RJ45 Console interface. To make the RJ45 Console cable, see *QSW-8200 Series Product Description*.
- Use the serial cable delivered with the QSW-8200 series switch when accessing through the USB Console interface.

Accessing through RJ45 Console interface

If you wish to access the QSW-8200 series switch on a PC through the RJ45 Console interface, connect the Console interface on the QSW-8200 series switch to the RS-232 serial interface on the PC, as shown in Figure 1-1. Then run the terminal emulation program such as Windows XP Hyper Terminal program on the PC to configure communication parameters as shown in Figure 1-2, and then log in to the QSW-8200 series switch.

Figure 1-1 Accessing device through PC connected with RJ45 Console interface

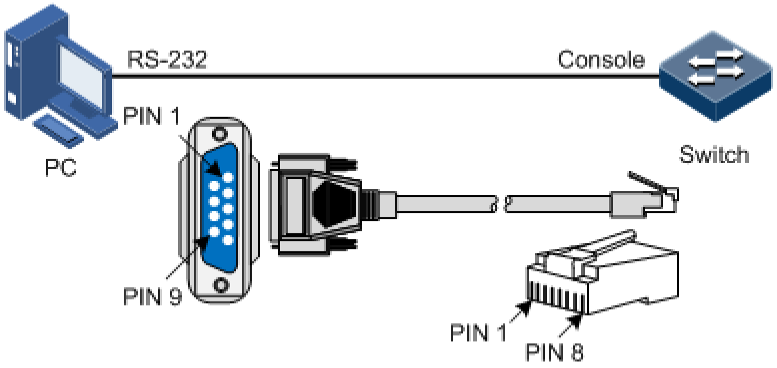
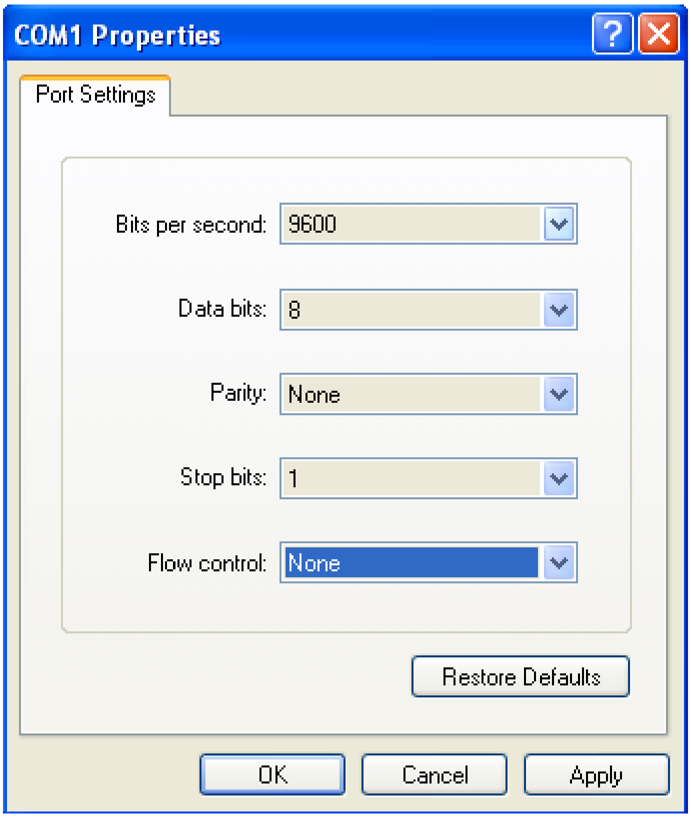


Figure 1-2 Configuring communication parameters in Hyper Terminal for RJ45 Console



Bits per second: 9600

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

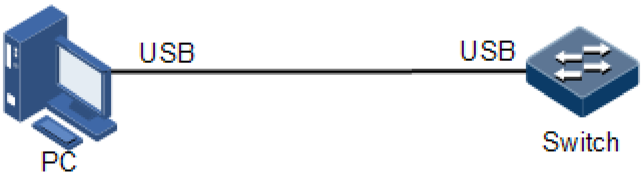
Note

Hyper Terminal is not available on Windows Vista or later Windows Operating Systems (OSs). For these OSs, download Hyper Terminal package and install it. This program is free for personal application.

Accessing through USB Console interface

When you wish to access the QSW-8200 series switch through the USB Console interface which connects to a PC, install the driver for converting the USB interface to the serial interface on the PC, and then use the USB Console cable to connect the USB interface on the QSW-8200 series switch with the USB interface on the PC, as shown in Figure 1-3.

Figure 1-3 Accessing device through PC connected with USB Console interface

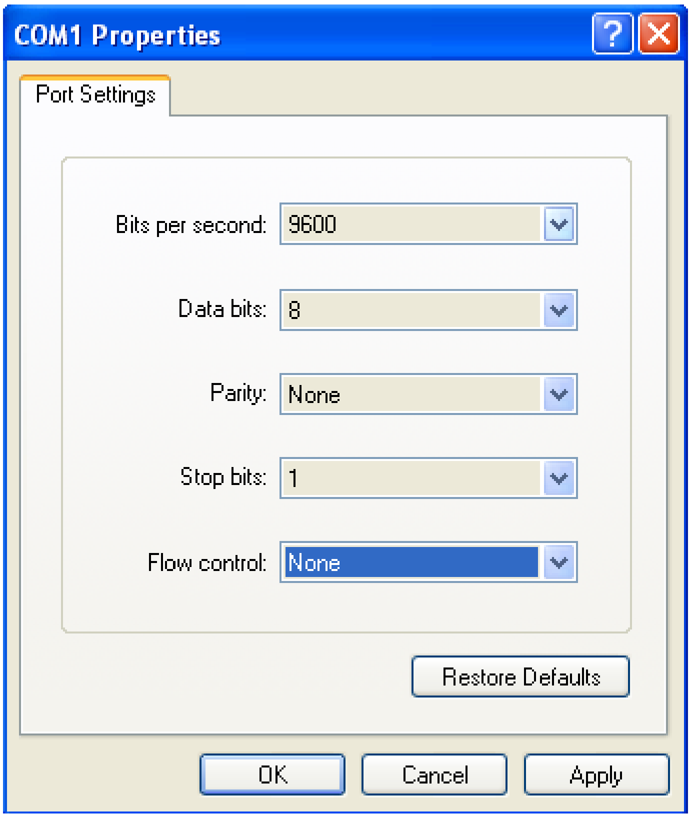


Note

- The driver for converting the USB interface to the serial interface is burnt on the CD-ROM delivered with user manuals. Install it in advance.
- Or you can download the driver from http://www.prolific.com.tw (choose the driver for model PL-2303).

Run the terminal emulation program such as Windows XP Hyper Terminal program on the PC to configure communication parameters as shown in Figure 1-4, and then log in to the QSW-8200 series switch.

Figure 1-4 Configuring communication parameters in Hyper Terminal for USB Console



Bits per second: 9600

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

Note

When configuring Hyper Terminal, choose a COM interface according to Ports (COM&LPT) in Device Manager in Windows OS.

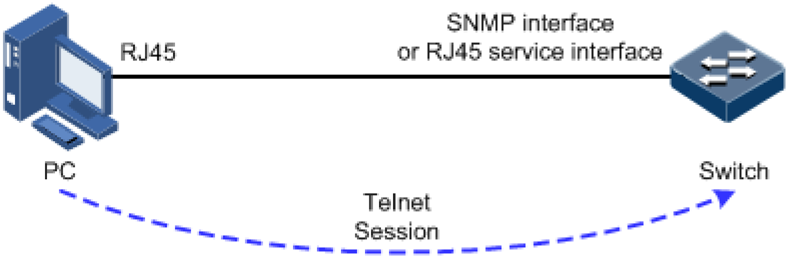
1.1.3 Accessing through Telnet

Use a PC to log in to the QSW-8200 series switch remotely through Telnet, log in to an QSW-8200 series switch from the PC at first, and then Telnet other QSW-8200 series switches on the network. Thus, you do not need to connect a PC to each QSW-8200 series switch.

Telnet features provided by the QSW-8200 series switch are as below:

- Telnet Server: run the Telnet client program on a PC to log in to the QSW-8200 series switch, and then configure and manage it. As shown in Figure 1-5, the QSW-8200 series switch provides the Telnet Server service in the case.

Figure 1-5 Networking with device as Telnet server



Before accessing the QSW-8200 series switch through Telnet, you need to log in to the QSW-8200 series switch through the Console interface and start the Telnet service.

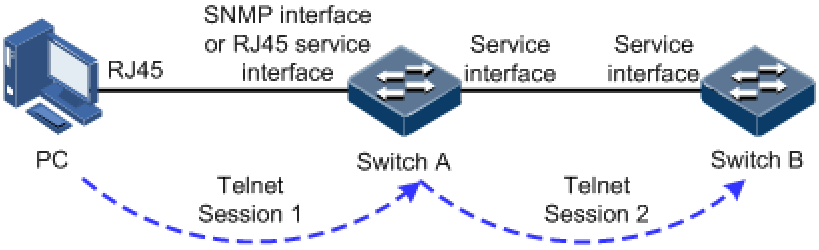
Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#interface ip if-number`	Enter Layer 3 interface configuration mode

3	`Qtech(config-ip)#ip address ip-address [ ip-mask ] [ vlan-id ]`
	`Qtech(config-ip)#quit`
		Configure the IP address for the QSW-8200 series switch and bind the VLAN of specified ID. The interface on which the Telnet service is started belongs to this VLAN.

4	`Qtech(config)#telnet-server accept port-list port-list`	(Optional) configure the interface that supports the Telnet feature.
5	`Qtech(config)#telnet-server close terminal-telnet session-number`	(Optional) disconnect the specified Telnet connection
6	`Qtech(config)#telnet-server max-session session-number`	(Optional) configure the maximum number of Telnet sessions.

- Telnet Client: when you connect to the QSW-8200 series switch through the PC terminal emulation program or Telnet client program on a PC, then telnet other QSW-8200 series switch devices and configure/manage them. As shown in Figure 1-6, Switch A provides both Telnet Server feature and Telnet Client feature.

Figure 1-6 Networking with device as Telnet client



Configure the Telnet Client device as below.

Step	Command	Description
1	`Qtech#telnet ip-address [ port port-id ]`	Log in other QSW-8200 series switch devices through Telnet.

1.1.4 Accessing through SSHv2

Telnet is lack of security authentication and it transports messages through Transmission Control Protocol (TCP) which exists with big potential security hazard. Telnet service may cause hostile attacks, such as Deny of Service (DoS), host IP deceiving, and routing deceiving.

The traditional Telnet and File Transfer Protocol (FTP) transmit password and data in plain text, which cannot satisfy users' security demands. SSHv2 is a network security protocol, which can effectively prevent the disclosure of information in remote management through data encryption, and provides greater security for remote login and other network services in network environment.

SSHv2 allows data to be exchanged through TCP and it builds up a secure channel over TCP. Besides, SSHv2 supports other service ports besides standard port 22, avoiding illegal attacks from the network.

Before accessing the QSW-8200 series switch through SSHv2, you must log in to the QSW-8200 series switch through the Console interface and start SSH service.

Default configurations for accessing the QSW-8200 series switch through SSHv2 are as follows.

Function	Default value
SSHv2 server status	Prohibit
Local SSHv2 key pair length of the device	512 bits
Authentication method of the device	Password
SSHv2 authentication timeout of the device	600s
Allowable failure number for SSHv2 authentication of the device	20
SSHv2 snooping port ID of the device	22
SSHv2 session status of the device	Enable

Configure SSHv2 service for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**generate ssh-key** *length*	Generate local SSHv2 key pair and designate its length.
3	Qtech(config)#**ssh2 server**	Start the SSHv2 server.
4	Qtech(config)#**ssh2 server authentication** { **password** | **rsa-key** | **tacacs** }	(Optional) configure SSHv2 authentication method.
5	Qtech(config)#**ssh2 server authentication public-key**	(Optional) use rsa-key authentication method to type the public key of clients to the QSW-8200 series switch.
6	Qtech(config)#**ssh2 server authentication-timeout** *period*	(Optional) configure SSHv2 authentication timeout. Authentication fails and the QSW-8200 series switch is disconnected when the time expires.
7	Qtech(config)#**ssh2 server authentication-retries** *times*	(Optional) configure retry times for SSHv2 authentication. Authentication will fail and the QSW-8200 series switch will be disconnected when the times exceed the upper limit.
8	Qtech(config)#**ssh2 server port** *port-id*	(Optional) configure SSHv2 snooping port ID. **Note** When you configure SSHv2 snooping port ID, the input parameter cannot take effect immediately until the SSHv2 service is restarted.
9	Qtech(config)#**ssh2 server session** *session-list* **enable**	(Optional) enable the SSHv2 session function.

1.1.5 Configuring Banner MotD

You can set the welcome message and prompt message before logging in to the terminal interface by Banner Message of the Day (MotD), such as influences of modifying configurations, alarm message, and exception clause. The message is shown in advance when you log in to the QSW-8200 series switch through the Hyper Terminal or Telnet.

Configure Banner MotD for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.

Step	Command	Description

2	`Qtech(config)#`**`banner motd`**
	`char`
	`message`
		Configure the prompt information to log in to the QSW-8200 series switch.
		• *char*: information separator, 1 Byte. You can input any characters except "?", while the beginning and ending characters must be the same.
		• *message*: prompt information. You can input up to 2560 characters.

3	`Qtech(config)#`**`banner-motd enable`**	Enable Banner MotD.

1.1.6 Managing users

When you start the QSW-8200 series switch for the first time, connect the PC through the Console interface to the QSW-8200 series switch, input the initial user name and password in HyperTerminal to log in and configure the QSW-8200 series switch.

Note

Initially, both the user name and password are Qtech.

If there is not any privilege restriction, any remote user can log in to the QSW-8200 series switch through Telnet or access the network by establishing PPP (Point to Point Protocol) connection when the Simple Network Management Protocol (SNMP) interface or other service interfaces of QSW-8200 series switch are configured with IP address. This is unsafe to the QSW-8200 series switch and network. So you need to manage login users by creating user name, password, and privilege on the QSW-8200 series switch.

Configure login user management for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`user name`** *`user-name`* **`password`** *`password`*	Create or modify the user name and password. Use the **no username** to delete an existing user.
2	`Qtech#`**`user name`** *`user-name`* **`privilege`** *`privilege-level`*	Configure login user privilege. The initial user privilege is 15, which is the highest privilege.
3	`Qtech#`**`user`** *`user-name`* `{` **`allow-exec`** `|` **`disallow-exec`** `}` *`first-keyword`* `[` *`second-keyword`* `]`	Configure the priority rule for login user to perform the command line. The specified **allow-exec** parameter allows you to perform commands higher than your privilege. The specified **disallow-exec** parameter allows you to perform commands lower than the current privilege only.

1.1.7 Checking configurations

Use the following commands to check the configuration results:

No.	Command	Description
1	`Qtech#show user [ detail ]`	Show the login user information.
2	`Qtech#show telnet-server`	Show Telnet Server configuration.
3	`Qtech#show ssh2 public-key [ authentication ]`	Show the public key used for SSHv2 authentication on the QSW-8200 series switch and client interface.
4	`Qtech#show ssh2 { server | session }`	Show information about SSHv2 server or session.
5	`Qtech(config)#show banner motd`	Show configurations of Banner MotD.

1.2 CLI

1.2.1 Introduction

The CLI is a medium for you communicating with the QSW-8200 series switch. You can configure, monitor, and manage the QSW-8200 series switch through the CLI.

You can log in to the QSW-8200 series switch through a terminal or a PC that runs terminal emulation program. Enter commands at the system prompt.

The CLI supports the following features:

- Configure the QSW-8200 series switch locally through the Console interface.
- Configure the QSW-8200 series switch locally or remotely through Telnet/Secure Shell v2 (SSHv2).
- Commands are classified into different levels. You can execute the commands that correspond to your level only.
- The commands available to you depend on which mode you are currently in.
- Keystrokes can be used to execute commands.
- Check or execute a historical command by checking command history. The last 20 historical commands can be saved on the QSW-8200 series switch.
- Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.
- The QSW-8200 series switch supports multiple intelligent analysis methods, such as fuzzy match and context association.

1.2.2 Levels

The QSW-8200 series switch uses hierarchy protection methods to divide command line into 16 levels from low to high.

- 0–4: visitor. Users can execute the **ping**, **clear**, and **history** commands, etc. in this level.

- 5–10: monitor. Users can execute the **show** command, etc.
- 11–14: operator. Users can execute commands for different services like Virtual Local Area Network (VLAN), Internet Protocol (IP), etc.
- 15: administrator. Users can execute basic command for operating the system.

1.2.3 Modes

Command line mode is the CLI environment. All system commands are registered in one (or some) command line mode. A command can be run in the corresponding mode only.

Establish a connection with the QSW-8200 series switch. If the QSW-8200 series switch is in default configuration, it will enter user EXEC mode, and the screen will display:

```
Qtech>
```

Input the **enable** command and correct password, and then enter privileged EXEC mode. The default password is Qtech.

```
Qtech>enable
Password:
Qtech#
```

In privileged EXEC mode, input the **config terminal** command to enter global configuration mode.

```
Qtech#config terminal
Qtech(config)#
```

Note

- The CLI prompts that Qtech is a default host name. You can modify it by executing the **hostname** *string* command in privileged EXEC mode.
- Commands executed in global configuration mode can also be executed in other modes. The functions vary with command modes.
- You can enter the **exit** or **quit** command to return to upper command mode. However, in privileged EXEC mode, you need to execute the **disable** command to return to user EXEC mode.
- You can execute the **end** command to return to privileged EXEC mode from any modes but user EXEC mode and privileged EXEC mode.

The QSW-8200 series switch supports the following command line modes.

Mode	Enter method	Description
User EXEC mode	Log in the device, input correct username and password	`Qtech>`

Mode	Enter method	Description
Privileged EXEC mode	In user EXEC mode, input the **enable** command and correct password.	`Qtech#`
Global configuration mode	In privileged EXEC mode, input the **config terminal** command.	`Qtech(config)#`
Physical layer interface configuration mode	In global configuration mode, input the **interface port** *port-id* command.	`Qtech(config-port)#`
Layer 3 interface configuration mode	In global configuration mode, input the **interface ip** *if-number* command.	`Qtech(config-ip)#`
VLAN configuration mode	In global configuration mode, input the **vlan** *vlan-id* command.	`Qtech(config-vlan)#`
Traffic classification configuration mode	In global configuration mode, input the **class-map** *class-map-name* command.	`Qtech(config-cmap)#`
Traffic policy configuration mode	In global configuration mode, input the **policy-map** *policy-map-name* command.	`Qtech(config-pmap)#`
Traffic policy configuration mode binding with traffic classification	In floe policy configuration mode, input the **class-map** *class-map-name* command.	`Qtech(config-pmap-c)#`
Access control list configuration mode	In global configuration mode, input the **access-list-map** *acl-number* { **deny** | **permit** } command.	`Qtech(config-aclmap)#`
Aggregation group configuration mode	In global configuration mode, input the **interface port-channel** *port-channel-number* command.	`Qtech(config-aggregator)#`
Service instance configuration mode	In global configuration mode, input **service** *cisid* **level** *level* command.	`Qtech(config-service)#`
EVC configuration mode	In global configuration mode, input the **ethernet evc** *evc-number evc-name* command.	`Qtech(config-evc)#`
MST region configuration mode	In global configuration mode, input the **spanning-tree region-configuration** command.	`Qtech(config-region)#`
Profile configuration mode	In global configuration mode, input the **igmp filter profile** *profile-number* command.	`Qtech(config-igmp-profile)#`

Mode	Enter method	Description
Cluster configuration mode	In global configuration mode, input the **cluster** command.	`Qtech(config-cluster)#`
Chinese alert mode	In any configuration mode, input the **language chinese** command.	`Qtech#`

1.2.4 Shortcut keys

The QSW-8200 series switch supports the following shortcut keys.

Shortcut key	Description
Up cursor key (↑)	Show previous command if there is any command input earlier; the display has no change if the current command is the earliest one in history records.
Down cursor key (↓)	Show next command if there is any newer command; the display has no change if the current command is the newest one in history records.
Left cursor key (←)	Move the cursor one character to left; the display has no change if the cursor is at the beginning of command.
Right cursor key (→)	Move the cursor one character to right; the display has no change if the cursor is at the end of command.
Backspace	Delete the character before the cursor; the display has no change if the cursor is at the beginning of command.
Tab	Press **Tab** after inputting a complete keyword, and the cursor will automatically appear a space to the end; press **Tab** again, and the system will show the follow-up inputting keywords. Press **Tab** after inputting an incomplete keyword, and the system automatically executes partial helps: • The system takes the complete keyword to replace input if the matched keyword is the one and only, and leaves one word space between the cursor and end of keyword; • In case of mismatch or matched keyword is not the one and only, display prefix at first, then press **Tab** to check words circularly, no space from cursor to the end of keyword, click **Space** key to input the next word; • If input incorrect keyword, press **Tab** will change to the next line and prompt error, the input keyword will not change.
Ctrl+A	Move the cursor to the beginning of the command line.
Ctrl+C	The ongoing command will be interrupted, such as **ping**, and **traceroute**.
Ctrl+D or **Delete**	Delete the character at the cursor.
Ctrl+E	Move the cursor to the end of the command line.

Shortcut key	Description
Ctrl+K	Delete all characters from the cursor to the end of the command line.
Ctrl+X	Delete all characters before the cursor (except cursor location).
Ctrl+Z	Return to privileged EXEC mode from the current mode (excluding user EXEC mode).
Space or **Y**	Scroll down one screen.
Enter	Scroll down one line.

1.2.5 Acquiring help

Complete help

You can acquire complete help under following three conditions:

- You can enter a question mark (?) at the system prompt to display a list of commands and brief descriptions available for each command mode.

```
Qtech>?
```

The command output is displayed as below.

```
clear     Clear screen
enable    Turn on privileged mode command
exit      Exit current mode and down to previous mode
help      Message about help
history    Most recent history command
language  Language of help message
list      List command
quit      Exit current mode and down to previous mode
terminal  Configure terminal
test    Test command
```

- After you enter a keyword, press **Space** and enter a question mark (?), all correlated commands and their brief descriptions are displayed if the question mark (?) matches another keyword.

```
Qtech(config)#ntp ?
```

The command output is displayed as below.

```
peer           Configure NTP peer
refclock-master  Set local clock as reference clock
server         Configure NTP server
```

- After you enter a keyword, press **Space** and enter a question mark (?), the value range and descriptions are displayed if the question mark (?) matches a parameter.

```
Qtech(config)#interface ip ?
```

The command output is displayed as below.

```
<0-14>  IP interface number
```

Incomplete help

You can acquire incomplete help under following three conditions:

- After you enter part of a particular character string and a question mark (?), a list of commands that begin with a particular character string is displayed.

```
Qtech(config)#c?
```

The command output is displayed as below.

```
class-map   Set class map
clear      Clear screen
cpu       Configure cpu parameters
create     Create static VLAN
```

- After you enter a command, press **Space**, and enter a particular character string and a question mark (?), a list of commands that begin with a particular character string is displayed.

```
Qtech(config)#show li?
```

The command output is displayed as below.

```
link-aggregation    Link aggregation
link-state-tracking  Link state tracking
```

- After you enter a partial command name and press **Tab**, the full form of the keyword is displayed if there is a unique match command. Otherwise, press **Tab** continuously to display different keywords and then you can select the required one.

Error message

The QSW-8200 series switch prints out the following error messages according to error type when you input incorrect commands.

Error message	Description
% " * " Incomplete command..	The input command is incomplete.
% Invalid input at '^' marked.	The keyword at the position marked by "^" is invalid or not existing.
Ambiguous input at '^' marked, follow keywords match it.	The keyword marked with "^" is unclear.
% Unconfirmed command.	The command input by you is not unique.
% Unknown command.	The command input by you does not exist.
% You Need higher priority!	Your priority is too low to execute the command.

Note

If there is error message mentioned above, use the CLI help information to solve the problem.

1.2.6 Display information

Display features

The CLI provides the following display features:

- The help information and prompt messages displayed at the CLI are in English.
- When messages are displayed at more than one screen, you can suspend displaying them with one of the following operations, as listed in Table 1-1.

Table 1-1 Shortcut keys for display feature

Shortcut key	Description
Press **Space** or **Y**	Scroll down one screen.
Press **Enter**	Scroll down one line.
Press any letter key (except **Y**)	Stop displaying and executing commands.

Filtering displayed information

The QSW-8200 series switch supports a series of commands starting with **show**, to check device configurations, operation and diagnostic information. Generally, these commands can output more information, and then user needs to add filtering rules to filter out unnecessary information.

The **show** command of the QSW-8200 series switch supports three kinds of filter modes:

- | **begin** *string*: show all lines starting from the assigned string.
- | **exclude** *string*: show all lines mismatching the assigned string.
- | **include** *string*: show all lines only matching the assigned string.

Page-break

Page-break is used to suspend displaying messages when they are displayed at more than one screen. After page-break is enabled, you can use shortcut keys listed in Table 1-1. If page-break is disabled, all messages are displayed when they are displayed at more than one screen.

By default, page-break is enabled.

Configure page-break for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`terminal page-break enable`**	Enable page-break.

1.2.7 Command history

The historical commands can be automatically saved at the CLI. You can use the up arrow (↑) or down arrow (↓) to schedule a historical command. By default, the last 20 historical commands are saved. You can set the number of commands to be saved at the CLI.

Configure command history for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech>`**`terminal history`** *`number`*	(Optional) configure the number of history commands saved in the system.
2	`Qtech>`**`enable`**	Enter privileged EXEC mode.
3	`Qtech#`**`history`**	Check the user history commands.

1.2.8 Restoring default value of command lines

The default value of command line can be restored by **no** option or **enable | disable** option.

- **no** option: be provided in front of a command and used to restore the default value, disable some feature, or delete a configuration. It is used to perform an operation that is opposite to the command. Therefore, the command with a **no** option is also called a reverse command.

- **enable | disable** option: be provided behind a command or in the middle of a command. The **enable** parameter is used to enable some feature or function while the **disable** parameter is used to disable some feature or function.

For example:

- In physical layer configuration mode, the **description** *text* command is used to modify descriptions about an interface while the **no description** command is used to delete descriptions about the interface and restore to the default values.
- In physical layer interface mode, the **shutdown** command is used to disable an interface while the **no shutdown** command is used to enable an interface.
- In global configuration mode, the **shutdown** command is used to disable an interface while the **no shutdown** command is used to enable an interface.
- In global configuration mode, the **terminal page-break enable** command is used to enable page-break while the **terminal page-break disable** command is used to disable terminal page-break.

Note

Most commands have default values, which are often restored by **no** option.

1.3 Managing files

1.3.1 Managing BootROM files

The BootROM file is used to boot the QSW-8200 series switch and finish device initialization. You can upgrade the BootROM file through File Transfer Protocol (FTP) FTP or Trivial File Transfer Protocol (TFTP). By default, the name of the BootROM file is bootrom or bootromfull.

After being powered on, the QSW-8200 series switch runs the BootROM file. When the system prompts "Press space into Bootrom menu", press **Space** to enter the Bootrom menu.

```
begin...

ram size:128M   testing...done

Init flash ...Done

Bootstrap_5.0.1.QSW-8200.1.20111018 Compiled Oct 18 2011, 17:26:52
Base Ethernet MAC address: 00:1f:ce:00:00:00



Press space into Bootstrap menu...
 0
```

You can perform the following operations in the menu.

Operation	Description
?	List all executable operations.
b	Quick execution for system bootrom software.
h	List all executable operations.
L	List all system startup software name and related information about the QSW-8200 series switch.
N	Set the Medium Access Control (MAC) address.
R	Reboot the device.
S	List all system startup software name and related information in the device and assign system startup software name loaded at the time of startup device.
T	Download and replace system startup software through TFTP.

1.3.2 Managing system files

System files are the files needed for system operation (like system startup software and configuration file). These files are usually saved in the memory. The QSW-8200 series switch manages them by a file system to facilitate user managing the memory. The file system can create, delete, and modify the file and directory.

In addition, the QSW-8200 series switch supports dual-system. There are 2 sets of system software saved at the memory. These 2 sets of system software are independent. When the QSW-8200 series switch fails to work due to upgrade failure, you can use another set to boot the QSW-8200 series switch.

Manage system files for the QSW-8200 series switch as below.

All the following steps are optional and in any sequence.

Step	Command	Description
1	Qtech#**download** { **bootstrap** | **system-boot** } { **ftp** | **sftp** }{ *ipv4-address* | *ipv6-address* } *user-name password file-name*	(Optional) download the BootROM file through FTP or SFTP.
2	Qtech#**download** { **bootstrap** | **system-boot** } **tftp** { *ipv4-address* | *ipv6-address* } *file-name*	(Optional) download the system startup file through TFTP.
3	Qtech#**download startup-config** { { **ftp** | **sftp** }{ *ipv4-address* | *ipv6-address* } *user-name password file-name* | **tftp** *ip-address file-name* } [**reservedevcfg**]	(Optional) upload the system startup file through FTP or SFTP.

1.4 Managing configuration files

The configuration file is a text file saving configuration CLIs. Through it, you can freely view and manage configurations of the QSW-8200 series switch.

1.4.1 Introduction

Type of configuration files

Configuration files are classified into the following two types:

- Startup configuration file: when the QSW-8200 series switch is started, it reads a file, which is called the startup configuration file (the factory configuration is loaded when the QSW-8200 series switch is started the first time). The startup configuration file is not lost upon power failure or restart.
- Running configuration file: when the QSW-8200 series switch is running, the file being used is the running configuration file. It contains the validated configurations made by the user during running. If it is not saved as the startup configuration file, it will be lost upon power failure or restart.

Note

Use the **show startup-config** command to show information about the startup configuration file. Use the **show running-config** command to show information about the running configuration file.

Before startup, the Flash saves the startup configuration file while the RAM saves nothing.

- During startup, the RAM reads the startup configuration file from the Flash, and generates a copy of the startup configuration file. Thus, the running configuration file is generated. The QSW-8200 series switch initializes itself with the copy of the startup configuration file, namely, the running configuration file.
- During running, any configurations that have taken effect are written into the running configuration file.

Format of configuration files

The configuration file has a suffix ".conf", and can be opened by the text book program in Windows OS. The contents are in the following format:

- Saved as Mode+Command format. Just keep the non-defaulted parameters to save space (see the command reference manual for default values of configuration parameters).
- Use the command mode for basic frame to organize commands. Put parameters of one mode together to form a section, and the sections are separated by the exclamation mark (!).
- The sequence of sections is: global configuration, logical interface configuration, physical interface configuration, protocol configuration, and so on.

For example:

```
System current configuration:
!command in view_mode
!
```

```
!command in config_mode first-step
link-aggregation load-sharing mode smac
lacp system-priority 3
lacp timeout fast
ip-access-list 0 deny ip any any
!
!command in aclmap_mode
!
!command in enable_mode
radius 192.168.0.2
radius-key "Qtech"
hostname 2800GF-A
!
!command in region_mode
!
!command in service_mode
!
!command in evc mode
!
!command in aggregation_mode
!
```

Location for storing configuration files

The configuration file can be saved in the following location:

- RAM (memory of the QSW-8200 series switch): the running configuration file is saved in the RAM, and lost upon power failure or restart.
- Flash (Flash memory of the QSW-8200 series switch): the startup configuration file is saved in the Flash, and will not be lost upon power failure or restart.

1.4.2 Preparing for configurations

Scenario

To restore the original startup configuration file or upgrade to the latest one, you can download it from the server. After modifying the current startup configuration file, upload original one to the server for backup.

Delete the startup configuration file under following situations:

- After software upgrade, the system software does not match the configuration file.
- The configuration file is corrupted.

Prerequisite

- The route between the QSW-8200 series switch and configuration terminal is reachable.
- The FTP server is available.

Note

Before using the FTP server, configure the user name and password. When uploading or downloading configuration files, input the user name and password specified on the FTP server.

1.4.3 Saving running configuration file

To make the current configurations take effect upon next restart, save the running configuration file as the startup configuration file.

Caution

When you save the running configuration file into the Flash, it overrides the original one. Thus, back up the original one before overriding.

Save the running configuration file for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**write**	Save the running configuration file into the Flash as the startup configuration file.

1.4.4 Uploading startup configuration file

Upload the startup configuration file for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**upload startup-config tftp tftp**{ *ip-address* | *ipv6-address* } *file-name*	Upload the startup configuration file from the Flash to the TFTP server.
2	Qtech#**upload startup-config** { **ftp** | **sftp** } { *ip-address* | *ipv6-address* } *user-name password file-name*	Upload the startup configuration file from the Flash to the FTP or Secure File Transfer Protocol (SFTP) server.

1.4.5 Downloading startup configuration file

Download the startup configuration file for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**download startup-config tftp** *ip-address file-name* [**reservedevcfg**]	Download the startup configuration file from the TFTP server to the Flash.
2	Qtech#**download startup-config** { **ftp** | **sftp** } *ip-address user-name password file-name* [**reservedevcfg**]	Download the startup configuration file from the FTP or SFTP server to the Flash.
3	Qtech#**reboot** [**in** *period* | **now**]	Restart the QSW-8200 series switch. The new startup configuration file will take effect.

1.4.6 Deleting configuration files

Delete the configuration file for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#dir`	Show information about files in the Flash.
2	`Qtech#erase [ file-name ]`	Delete the configuration file in the Flash. If you do not specify *file-name*, the startup configuration file will be deleted.

Note

- The suffix of the configuration file does not indicate anything. It is ".conf".
- After the startup configuration file is deleted, the QSW-8200 series switch will use the factory settings for initialization.

1.4.7 Checking configurations files

Use the following commands to check configuration results.

Step	Command	Description
1	`Qtech#show running-config`	Show the running configuration file.
2	`Qtech#show startup-config`	Show the startup configuration file.

1.5 Time management

1.5.1 Configuring time and time zone

To coordinate the QSW-8200 series switch to work well with other devices, you must configure system time and time zone accurately.

The QSW-8200 series switch supports 3 system time modes, which are time stamp mode, auxiliary time mode, and default mode from high to low according to timing unit accuracy. You need to select the most suitable system time mode manually in accordance with actual application environment.

Default configurations of time and time zone are as below.

Function	Default value
System time	2000-01-01 08:00:00.000
System time mode	Default
System belonged time zone	UTC+8

Function	Default value
Time zone offset	+08:00
Functional status of Daylight Saving Time	Disable

Configure time and time zone for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**clock set** *hour minute second year month day*	Configure system time.
2	Qtech#**clock timezone** { **+** | **-** } *hour minute timezone-name*	Configure the system time zone.

1.5.2 Configuring DST

Daylight Saving Time (DST) is a kind of artificial regulation local time system for saving energy. At present, there are nearly 110 countries operating DST every summer around the world, but different countries have different stipulation for DST. Thus, you should consider the local conditions when configuring DST.

Configure DST for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**clock summer-time enable**	Enable DST.
2	Qtech#**clock summer-time recurring** { *week* | **last** } { **fri** | **mon** | **sat** | **sun** | **thu** | **tue** | **wed** } *month hour minute* { *week* | **last** } { **fri** | **mon** | **sat** |**sun** | **thu** | **tue** | **wed** } *month hour minute offset-mm*	Configure calculation period for system DST.

Note

- When you configure the system time manually, if the system uses DST, such as DST from 2 a.m. on the second Sunday, April to 2 a.m. on the second Sunday, September every year, you have to advance the clock one hour faster during this period, that is, set the time offset as 60min. So the period from 2 a.m. to 3 a.m. on the second Sunday, April each year is inexistent. Configuring time manually in this period will fail.
- The DST in southern hemisphere is opposite to the northern hemisphere, which is from September to April next year. If the start time is later than end time, the system will suppose that it is in the southern hemisphere. That is to say, the DST is the period from the start time this year to the end time next year.

1.5.3 Configuring NTP

Network Time Protocol (NTP) is a time synchronization protocol defined by RFC1305, used to synchronize time between the distributed time servers and clients. NTP transmits data based on UDP, using UDP port 123.

The purpose of NTP is to synchronize all clocks in a network quickly and then the QSW-8200 series switch can provide different application over a unified time. Meanwhile, NTP can ensure very high accuracy, with accuracy of 10ms around.

The QSW-8200 series switch in support of NTP cannot only receive synchronization from other clock source, but also to synchronize other devices as a clock source.

The QSW-8200 series switch adopts multiple NTP working modes for time synchronization:

- Server/Client mode

In this mode, the client sends clock synchronization messages to different servers. The servers work in server mode automatically after receiving the synchronization message and sending response messages. The client receives response messages, performs clock filtering and selection, and is synchronized to the preferred server.

In this mode, the client can be synchronized to the server but the server cannot be synchronized to the client.

- Symmetric peer mode

In this mode, the active equity sends a clock synchronization message to the passive equity. The passive equity works in passive mode automatically after receiving the message and sends the answering message back. By exchanging messages, the two equities build up the symmetric peer mode. The active and passive equities in this mode can synchronize each other.

Default configurations of NTP are as below.

Function	Default value
Whether the device is the NTP master clock	No
Global NTP server	Inexistent
Global NTP symmetric peer	Inexistent
Reference clock source	0.0.0.0

Configure NTP for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**ntp server** *ip-address* [**version** [**v1** | **v2** | **v3**]]	(Optional) configure NTP server address for client device working in server/client mode.
3	Qtech(config)#**ntp peer** *ip-address* [**version** [**v1** | **v2** | **v3**]]	(Optional) configure NTP equity address for the QSW-8200 series switch working in equity mode.

Step	Command	Description
4	`Qtech(config)#ntp refclock-master [ ip-address ] [ stratum ]`	Configure clock of the QSW-8200 series switch as NTP reference clock source for the QSW-8200 series switch.
5	`Qtech(config)#ntp poll-interval number`	(Optional) configure the NTP synchronization internal in stable synchronization status.

Note

If the QSW-8200 series switch is configured as the NTP reference clock source, it cannot be configured as the NTP server or NTP symmetric peer; vice versa.

1.5.4 Configuring SNTP

Simple Network Time Protocol (SNTP) is used to synchronize the system time of the QSW-8200 series switch with the time of the SNTP device on the network. The time synchronized by SNTP protocol is Greenwich Mean Time (GMT), which can be translated into the local time according to system settings of time zone.

Default configurations of SNTP are as below.

Function	Default value
IP address of the SNTP server	Inexistent

Configure SNTP for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#sntp server ip-address`	(Optional) configure the IP address of the SNTP server for the client device working in server/client mode.

Note

After configuring the IP address of the SNTP server, the QSW-8200 series switch tries to obtain clock information from the SNTP server every 3s, and the maximum timeout for clock information is 10s.

1.5.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Qtech#show clock [ summer-time recurring ]`	Show configurations of the system time, time zone and DST.
2	`Qtech#show sntp`	Show SNTP configurations.
3	`Qtech#show ntp status`	Show NTP configurations.
4	`Qtech#show ntp associations`	Show information about NTP connection.

1.6 Interface management

1.6.1 Introduction

Ethernet is a very important LAN networking technology which is flexible, simple and easy to implement. The Ethernet interface includes the Ethernet electrical interface and Ethernet optical interface.

The QSW-8200 series switch supports both Ethernet electrical and optical interfaces.

Auto-negotiation

Auto-negotiation is used to make the devices at both ends of a physical link automatically choose the same working parameters by exchanging information. The auto-negotiation parameters include duplex mode, interface rate, and flow control. Once successful in negotiation, the devices at both ends of the link can work in the same duplex mode and interface rate.

Cable connection

Generally, the Ethernet cable can be categorized as the Medium Dependent Interface (MDI) cable and Medium Dependent Interface crossover (MDI-X) cable. MDI provides physical and electrical connection from terminal to network relay device while MDI-X provides connection between devices of the same type (terminal to terminal). Hosts and routers use MDI cables while hubs and switches use MDI-X interfaces. Usually, the connection of different devices should use the MDI cable while devices of the same type should use the MDI-X cable. Devices in auto-negotiation mode can be connected by the MDI or MDI-X cable.

The Ethernet cable of the QSW-8200 series switch supports MDI/MDI-X auto-negotiation.

1.6.2 Default configurations of interfaces

Default configurations of physical layer interface are as below.

Function	Default value
MTU on the interface	1526 Bytes
Duplex mode of interfaces	Auto-negotiation
Interface rate	Auto-negotiation

Function	Default value
Flow control status on the interface	Disable
Combo interface optical/electrical mode	Auto-selection mode
Flow control status on the Combo interface	Disable
Time interval of interface dynamic statistics	2s
Interface status	Enable

1.6.3 Configuring basic attributes of interface

The interconnected devices cannot communicate normally if their interface attributes (such as MTU, duplex mode, and rate) are inconsistent. Then you have to adjust interface attributes to make the devices at both ends match each other.

Configure basic attributes of interface for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`system mtu`** *`size`*	Configure the Maximum Transmission Unit (MTU) for all interfaces. MTU is the maximum number of Bytes allowed to pass on the interface (without fragment). When the length of the forwarded packet exceeds the maximum value, the QSW-8200 series switch will discard this packet automatically.
3	`Qtech(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
4	`Qtech(config-port)#`**`duplex`** `{` **`auto`** `|` **`full`** `|` **`half`** `}`	Configure interface duplex mode. Ethernet physical layer has half-duplex, full-duplex and auto-negotiation modes. • In half-duplex mode, the interface can only receive or send packet at any time • In full-duplex mode, the interface can both receive and send packet at any time Auto-negotiation indicates that the two devices at both ends of a link can exchange packets and select duplex mode automatically. Once negotiation successful, the two devices can transmit packets in the same duplex mode. By default, the interface duplex mode is auto-negotiation.

Step	Command	Description
5	Qtech(config-port)#**speed** { **auto** | **10** | **100** | **1000** }	Configure the interface rate. For optical interfaces, the interface rate depends on specifications of the optical module. **Note** The GE interface supports being configured with **speed 10000**.

1.6.4 Configuring flow control on interfaces

IEEE 802.3x is a flow control method for full duplex on the Ethernet data layer. When the client sends request to the server, it will send the PAUSE frame to the server if there is system or network jam. Then, it delays data transmission from the server to the client.

Configure flow control on interfaces for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**flowcontrol** { **receive** | **send** } { **off** | **on** }	Enable/Disable flow control over 802.3x packets on the interface. By default, flow control is disabled on the interface.

1.6.5 Configuring Combo interface

The Combo interface on the QSW-8200 series switch supports both optical modules and electrical modules, so transmission media can be optical fiber or cables according to interface media type supported by the peer device. If both two kinds of transmission media for connection are used, service transmission can only use one of them at the same time.

The Combo interface selects transmission medium in two modes: mandatory and automatic. If the configuration mode is automatic and two kinds of transmission medium of optical fiber and cable connections are normal, the interface will automatically choose one of them as an effective transmission line as well as automatically select the other for service transmission when the current one fails.

In auto-selection mode, after the Combo optical interface and Combo electrical interface are configured respectively, the device automatically use the optical/electrical interface if needed, without configuring them every time upon use.

Configure the Combo interface for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Qtech(config-port)#`**`media type`** `{` **`auto`** `|` **`fiber`** `|` **`copper`** `}`	Configure the optical/electrical mode for the Combo interface. ● **auto**: automatic selection mode ● **fiber**: force to use optical interface. ● **copper**: force to use electrical interface.
4	`Qtech(config-port)#`**`description media-type`** `{` **`fiber`** `|` **`copper`** `}` *`word`*	Configure description of optical/electrical attributes of the Combo interface.
5	`Qtech(config-port)#`**`speed`** `{` **`auto`** `|` **`10`** `|` **`100`** `|` **`1000`** `|` **`10000`** `}`	Configure the optical/electrical transmission rate of the Combo interface. The interface rate also depends on specifications of the selected module.
6	`Qtech(config-port)#`**`duplex`** `{` **`auto`** `|` **`full`** `|` **`half`** `}`	Configure Combo interface optical/electrical duplex mode.
7	`Qtech(config-port)#`**`mdi`** `{` **`auto`** `|` **`normal`** `|` **`xover`** `}`	Configure MDI mode of the electrical Combo interface.
8	`Qtech(config-port)#`**`flowcontrol media-type`** `{` **`fiber`** `|` **`copper`** `}` `[` **`send`** `|` **`receive`** `]` `{` **`on`** `|` **`off`** `}`	Configure optical/electrical bi-direction or Rx/Tx flow control for the Combo interface.

1.6.6 Configuring interface statistics

Configure interface statistics for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`dynamic statistics time`** *`period`*	Configure interface dynamic statistics time interval. By default, the dynamic statistics is taken every 2s on the interface.
3	`Qtech(config)#`**`clear interface port-list`** *`port-list`* **`statistics`**	Clear the interface statistics saved on the QSW-8200 series switch.

1.6.7 Enabling/Disabling interface

Enable/Disable an interface for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Qtech(config-port)#`**`shutdown`**	Disable the current interface. By default, the interface is enabled. Use the **no shutdown** command to re-enable the disabled interface.

1.6.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Qtech#`**`show interface port-list`** *`port-list`*	Show interface status.
2	`Qtech#`**`show interface port-list`** *`port-list`* **`statistics`**	Show interface statistics.
3	`Qtech#`**`show interface port-list`** *`port-list`* **`flowcontrol`**	Show interface flow control.
4	`Qtech#`**`show system mtu`**	Show system MTU.
5	`Qtech#`**`show combo description port-list`** [*`port-list`*]	Show description of the Combo interface.
6	`Qtech#`**`show combo configuration port-list`** [*`port-list`*]	Show configurations of the Combo interface.

1.7 Configuring basic information

Configure basic information about the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`hostname`** *`name`*	(Optional) configure the device name. By default, the device name is Qtech. The system supports changing device name to make users distinguish different devices on the network. Changing device name take effect immediately, which can be seen in terminal prompt.

Step	Command	Description
2	`Qtech#language { chinese | english }`	(Optional) configure language mode. By default, the language is English. The system supports displaying help and prompt information in both English and Chinese.
3	`Qtech#write`	Save configurations. Save configurations to the QSW-8200 series switch after configuration, and the new saved configurations will overwrite the original configuration. Without being saved, the new configuration will be lost after rebooting, and the QSW-8200 series switch will continue working with the original configuration. **Note** Use the **erase file-name** command to delete the configuration file. This operation cannot be rolled back, so use this command with care.
4	`Qtech#reboot [ in` *`period`* `| now ]`	**Caution** Rebooting the QSW-8200 series switch will interrupt services, so do this with care. Save the configuration before rebooting to avoid losing configurations. (Optional) configure reboot options. When the QSW-8200 series switch fails, reboot it to try to solve the problem according to actual condition.

1.8 Configuring management and auxiliary interfaces

1.8.1 Configuring SNMP interface

You can configure the IP address of the SNMP interface to connect the QSW-8200 series switch to the NMS or use Telnet login from the SNMP interface to achieve the connection between the QSW-8200 series switch and the NMS, the QSW-8200 series switch and user PC.

Configure the SNMP interface for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#management-port ip address` *`ip-address`* `[` *`ip-mask`* `]`	Configure the IP address of the SNMP interface.
3	`Qtech(config)#management-port dhcp server { enable`	Enable DHCP Server on the SNMP interface.

Step	Command	Description

4	`Qtech(config)#exit`
	`Qtech#show management-port ip-address`
		Show configurations of the IP address of the SNMP interface.

5	`Qtech#show management-port dhcp server`	Show status of DHCP Server on the SNMP interface.

1.8.2 Configuring Console interface

Configure the Console interface for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#console open`	(Optional) enable the Console interface. Use this command in non-Console command lines only. ⚠ **Caution** Using the **console close** command to disable the Console interface causes the QSW-8200 series switch to be out of control. Use it with care.
3	`Qtech(config)#login-trap enable`	(Optional) enable sending Trap upon user login or exit.

1.9 Configuring task scheduling

When you need to use some commands periodically or at a specified time, configure task scheduling.

The QSW-8200 series switch supports realizing task scheduling by combining the program list to command lines. You just need to specify the start time of the task, period, and end time in the program list, and then bind the program list to command lines to realize the periodic execution of command lines.

Configure task scheduling for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.

Step	Command	Description
2	Qtech(config)#**schedule-list** *list-number* **start** { **date-time** *mm-dd-yyyy hh*:*mm*:*ss* [**every** { **day** | **week** | *period hh*:*mm*:*ss* }] **stop** *mm-dd-yyyy hh*:*mm*:*ss* | **up-time** *period hh*:*mm*:*ss* [**every** *period hh*:*mm*:*ss*] [**stop** *period hh*:*mm*:*ss*] }	Create a scheduling list, and configure it.
3	Qtech(config)#*command-string* **schedule-list** *list-number*	Bind the command line which needs periodic execution and supports scheduling list to the scheduling list.
4	Qtech#**show schedule-list** [*list-number*]	Show configurations of the scheduling list.

1.10 Watchdog

External electromagnetic field interferes with the working of single chip microcomputer, and causes program fleet and dead circulation so that the system cannot work normally. Considering the real-time monitoring of the running state of single chip microcomputer, a program is specially used to monitor the running status of switch hardware, which is commonly known as the Watchdog.

The QSW-8200 series switch will be rebooted when it fails due to task suspension or dead circulation, and without feeding the dog within a feeding dog cycle.

The Watchdog function can prevent the system program from dead circulation due to uncertain fault, thus improving stability of the system.

Configure Watchdog for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**watchdog enable**	Enable Watchdog. Use the **watchdog disable** command to disable this function.
2	Qtech#**show watchdog**	Show Watchdog status.

1.11 Auto-loading

1.11.1 Introduction

Traditionally, configuration files are loaded by the serial interface, which takes a long time, is loaded at a low rate, and fails to support remote loading. Auto-loading modes, such as FTP and TFTP, can solve those problems.

The QSW-8200 series switch supports TFTP auto-loading mode.

TFTP auto-loading means that users obtain configuration files from the server to the QSW-8200 series switch, and then configure the QSW-8200 series switch. Auto-loading allows configuration files to contain related commands for multiple configuration loadings to meet file auto-loading requirements in complex network environment.

When configuring auto-loading, specify the name of the file to be automatically loaded in the following ways:

- Obtaining the file name from the DHCP server to the DHCP client (QSW-8200 series switch)
- Manually specifying
- Specifying the naming convention: determining the file name by attributes of the QSW-8200 series switch (such as device model, MAC address, and software version).

Note

During auto-loading, the priorities of the previous three ways are in ascending order.

The naming convention number is composed of 5 digits, and ranges from 80001 to 89999. Figure 1-7 and Table 1-2 describe naming convention rules.

Figure 1-7 Naming convention for auto-loading

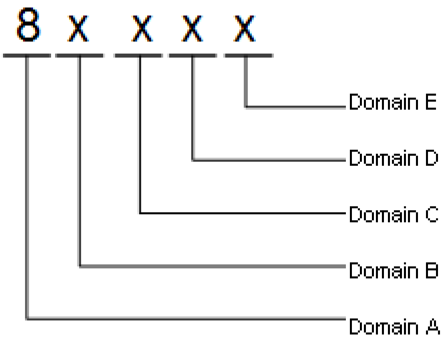


Table 1-2 Naming convention for auto-loading rules

Domain	Meaning	Value	Description
A	–	8	No special meaning
B	Device model	0–9	• 0: the file name does not contain the device model. • 1: the file name contains the device model. • 2–9: reserved for extended rules

Domain	Meaning	Value	Description
C	MAC address rule	0–9	Take 001F.CE08.5118 for example: • 0: the file name does not contain the MAC address. • 1: the file name contains the first 2 characters of the MAC address, namely, containing "00". • 2: the file name contains the first 4 characters of the MAC address, namely, containing "000E". • 3: the file name contains the first 6 characters of the MAC address, namely, containing "001F.CE". • 4: the file name contains the first 8 characters of the MAC address, namely, containing "001F.CE08". • 5: the file name contains the first 10 characters of the MAC address, namely, containing "001F.CE08.51". • 6: the file name contains all characters of the MAC address, namely, containing "001F.CE08.5118". • 7–9: reserved for extended rules
D	Software version rule	0–9	Take QSW-8200_REAP_1.2.278_2014022 for example: • 0: the file name does not contain software version. • 1: the file name contains complete software version, namely, containing "QSW-8200_REAP_1.2.278_2014022". • 2: the file name contains complete software version excluding device model, namely, containing "REAP_1.2.278_2014022". • 3: the file name contains complete software version excluding device model and date, namely, containing "REAP_1.2.278". • 4: the file name contains the first 3-digit software version, namely, containing "REAP_1.2.278". • 5: the file name contains the first 2-digit software version, namely, containing "REAP_1.2". • 6: the file name contains the first 1-digit software version, namely, containing "REAP_1". • 7–9: reversed for rule expansion
E	Extended rule	0–9	• 0: not supporting extended rules • 1–9: reserved for extended rules

The file name with the previous naming conventions is in the following format:

(device model)_M(MAC address)_(software version)

For example, rule 81650 indicates a file name of:

QSW-8200_M001F.CE08.5118_REAP_1.2

1.11.2 Preparing for configurations

Scenario

The QSW-8200 series switch needs to update the configuration file through TFTP auto-loading.

Prerequisite

A TFTP environment is established to make the QSW-8200 series switch and TFTP server reachable.

1.11.3 Configuring auto-loading

Caution

- The file version is "year-month-day-time", which is automatically generated during loading and needless of your configuration.
- After the system startup file and system bootstrap file are automatically loaded, the QSW-8200 series switch will be restarted to make these files take effect. Thus, you must configure local file overriding in advance.

Configuring naming convention through CLI

Configure naming convention through CLI for the QSW-8200 series switch as below.

No.	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**service config tftp-server** *ip-address*	Configure the IP address of the TFTP server. By default, it is not configured.
3	Qtech(config)#**service config filename rule** [*rulenumber* [**prefix** *prefix*] [**postfix** *postfix*]]	Configure naming convention for files. By default, it is not configured. The QSW-8200 series switch uses the default file name "startup_config.conf".
	Qtech(config)#**service config filename** *file-name*	Specify the name of the file to be loaded.
4	Qtech(config)#**service config version startup-config** *version*	(Optional) configure the file version.
5	Qtech(config)#**service config overwrite enable**	(Optional) enable local file overriding.
6	Qtech(config)#**service config**	Enable auto-loading.
7	Qtech(config)#**service config trap enable**	(Optional) enable sending Trap upon updating file.

Note

- For auto-loading, the priority of configuring the IP address through CLI is higher than that of obtaining the IP address as a DHCP client.
- If local file overriding is not enabled, the startup configuration file to be loaded will be lost after reboot.

Configuring naming convention through DHCP

Configure naming convention through DHCP for the QSW-8200 series switch as below.

No.	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**service config overwrite enable**	(Optional) enable local file overriding.
3	Qtech(config)#**service config**	Enable auto-loading.
4	Qtech(config)#**service config trap enable**	(Optional) enable sending Trap upon updating file.

Note

The file name must comply with the resolution rules of the DHCP server.

1.11.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show service config**	Show information about configured auto-loading.
2	Qtech#**show service config filename rule** [*rulenumber* [**prefix** *prefix*] [**postfix** *postfix*]]	Show naming convention for files.

1.12 Software upgrade

1.12.1 Introduction

System software includes BootROM and system software:

- BootROM: used to guide and initialize the QSW-8200 series switch.
- System software: used to provide drivers for hardware and guide the QSW-8200 series switch to enter CLI.

Note

The device that supports dual systems can save two sets of system software simultaneously in the memory. When software upgrade fails and consequently the QSW-8200 series switch crashes, you can use another version of system software to start the QSW-8200 series switch.

To add a new feature, optimize existing functions, or clear a bug of the current software version, you can upgrade the device software.

Software upgrade contains the following two types:

- Upgrade through BootROM
- Upgrade through CLI

1.12.2 Preparing for configurations

Scenario

Software upgrade is required.

Prerequisite

A TFTP/FTP environment is established to make the QSW-8200 series switch and TFTP/FTP server reachable.

1.12.3 Upgrading system software through BootROM

Note

Only when software upgrade through CLI is unavailable can you use this method. This method is not recommended.

Step	Command

1	Log in the QSW-8200 series switch through the serial interface as the administrator, enter Privileged EXEC mode, and reboot the QSW-8200 series switch by the **reboot** command.
	`Qtech#`**`reboot`**
	`Please input 'yes' to confirm: `**`yes`**
	`Rebooting ...`
	`begin...`
	`ram size: 256M   testing...done`
	`Init flash ...Done`
	`QSW-8200_Bootstrap_5.1.1_20121123, Qtech Compiled May 26 2012,12: 44: 09`
	`Base Ethernet MAC address: 00: 1f: ce: 00: 00: 00`
	`Press space into Bootstrap menu...`
	` 0`

<table>
<tr><th>Step</th><th>Command</th></tr>
<tr><td>2</td><td>

Click **Space** key to enter the **Qtech** interface when the system displays "Press space into Bootstrap menu...", then input "?" to display command list:

```
                    BIG BOOT
                  8200_Bootstrap_5.1.1_20121129(22:47:01)
 ?                 - List all available commands
 h                 - List all available commands
 V                 - Show bootstrap version
 b                 - Boot an executable image
 T                 - Download system program
 u                 - XMODEM download system boot image
 S                 - select boot system sofware
 R                 - Reboot
```

Caution

The input letters are case sensitive.

</td></tr>
<tr><td>3</td><td>

Input "T" to download the system boot file through FTP and replace it, the displayed information is as below.

```
[Qtech]:T
Index    Name                              Size
----------------------------------------------------------
1*      QSW-8200-28F_REAP_1.2.52_20121210       536bf3
2       -----------                        0
Current selected version is 1
Please select a version to overwrite:1

dev name: QSW-8200-28F-4C
unit num:1
file name: system_boot.Z QSW-8200-28F_REAP_1.2.52_20121210
local ip: 192.168.1.1 192.168.18.250
server ip: 192.168.1.2 192.168.18.33
user:1
password:123456
Loading...  Done
Saving file to flash...  Done
```

Caution

Ensure the input file name here is correct. The file name should not be longer than 80 characters.

Local IP is the IP address of the QSW-8200 series switch, and the server IP is the IP address of the PC. They must be in the same network segment.

</td></tr>
<tr><td>4</td><td>

Input "b" to quickly execute the bootstrap file, reboot the QSW-8200 series switch, and load the downloaded system boot file.

</td></tr>
</table>

Commands in the BootROM menu are described as below.

Command	Description
?	List all available operations.

	`u - XMODEM download system boot image`
	`S - select boot system sofware`
	R - Reboot

h	List all available operations.
V	Show BootStrap version.
b	Fast execute the system bootstrap file.
T	Download the system startup file.
u	Download system startup file through the XMODEM protocol.
S	Choose a version of system software to be started.
R	Restart the QSW-8200 series switch.

1.12.4 Upgrading system software through CLI

Before upgrading system software through CLI, you should establish a FTP/SFTP/TFTP environment, take a PC as the FTP/SFTP/TFTP server and the QSW-8200 series switch as the client, and make the PC and QSW-8200 series switch reachable.

No.	Command	Description
1	Qtech#**download bootstrap** { { **ftp** | **sftp** } [*ip-address user-name password file-name*] | **tftp** [*ip-address file-name*] }	Download the system bootstrap file through FTP/SFTP/TFTP.
2	Qtech#**download system-boot** { { **ftp** | **sftp** } [*ip-address user-name password file-name*] | **tftp** [*ip-address file-name*] }	Download the system boot file through FTP/SFTP/TFTP.
3	Qtech#**reboot** [**in** *period* | **now**]	Restart the QSW-8200 series switch. It will automatically load the downloaded system boot file.

1.12.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show version**	Show system version information.

1.13 Configuration examples

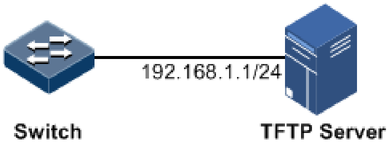
1.13.1 Exampe for configuring TFTP auto-loading

Networking requirements

As shown in Figure 1-8, connect the TFTP server with the Switch, configure auto-loading function on the switch to make the switch automatically load configuration file from TFTP server. Hereinto, the IP address of the TFTP server is 192.168.1.1 and the naming convention for configuration file name meet the following conditions:

- The device model is included in the name of the configuration file.
- The complete MAC address is included in the name of the configuration file.
- First 2 digits of software version are included in the name of the configuration file.
- No extension rules are supported.

Figure 1-8 Configuring auto-loading



Configuration steps

Step 1 Configure the IP address of the TFTP server.

```
Qtech#config
Qtech(config)#service config tftp-server 192.168.1.1
```

Step 2 Configure naming convention for the file name.

```
Qtech(config)#service config filename rule 81650
```

Step 3 Configure the file name.

```
Qtech(config)#service config filename ABC
```

Step 4 Enable overwriting local configuration file.

```
Qtech(config)#service config overwrite enable
```

Step 5 Enable auto-loading configuration.

```
Qtech(config)#service config
```

Checking results

Use the **show service config** command to show auto-loading configurations.

```
Qtech(config)#show service config
  Auto upgrade :                    enable
  Config server IP address:           192.168.1.1
  Config filename rule:               81650
  Config file name:                   ABC
  System boot file version:           1107290
  Bootstrap flie version :            :48:050
  Startup-config file version:        0000000
  Overwrite local configuration file:  enable
  Send Completion trap:                disable
  Current File Type:                  none
  Operation states:                   done
  Result:                             none
```

2 Ethernet

This chapter describes basic principles and configurations of Ethernet, and provides related configuration examples, including the following sections:

- MAC address table
- VLAN
- Customer VLAN
- QinQ
- VLAN mapping
- STP
- RSTP/MSTP
- Interface protection
- Port mirroring
- L2CP
- Layer 2 protocol transparent transmission
- GARP

2.1 MAC address table

2.1.1 Introduction

The MAC address table records mappings between MAC addresses and interfaces. It is the basis for an Ethernet device to forward packets. When the Ethernet device forwards packets on Layer 2, it searches the MAC address table for the forwarding interface, implements fast forwarding of packets, and reduces broadcast traffic.

The MAC address table contains the following information:

- Destination MAC address
- Destination MAC address related interface number
- Interface belonged VLAN ID
- Flag bits

Classification of MAC address entries

The MAC address table contains static address entries and dynamic address entries.

- Static MAC address entry: also called the permanent address, added and removed by the user manually, not aged with time. For a network with stable topology, adding static address entries manually can reduce broadcast traffic. The priority of static MAC address entries is higher than that of dynamic MAC address entries, which prevents unauthorized users to access the network by forging themselves as authorized users, and improves network security. After configurations are saved, static MAC address entries will not be lost even though the QSW-8200 series switch is restarted.

Note

Blackhole MAC address entry: a special type of static MAC address entry. When the destination or source MAC address of a packet matches the blackhole MAC address, the packet will be discarded.

- Dynamic MAC address entry: added by the QSW-8200 series switch through MAC address learning, aged according to the configured aging time, and automatically updated by the QSW-8200 series switch, and making the QSW-8200 series switch better adapt to network changes. After the QSW-8200 series switch is restarted, dynamic MAC address entries will be lost.

MAC address forwarding modes

Ethernet device adopts following forwarding modes according to MAC address entry:

- Unicast: when a MAC address entry, related to the destination MAC address of a packet, is listed in the MAC address table, the QSW-8200 series switch will directly forward the packet to the receiving interface through the egress port of the MAC address entry. If the entry is not listed, the QSW-8200 series switch broadcasts the packet to other devices.
- Broadcast: when the QSW-8200 series switch receives a packet with an all-F destination address, or its MAC address is not listed in the MAC address table, the QSW-8200 series switch forwards the packet to all ports except the port that receives this packet.

Dynamic MAC address entry learning

Dynamic MAC address entries can be learned through the dynamic MAC address entry learning mechanism. For example, port 1 on the QSW-8200 series switch receives packets from VLAN 2 of PC A. The QSW-8200 series switch checks whether there are entries of MAC A+VLAN 2+port 1:

Aging time of dynamic MAC address entries

There is limit on the capacity of the MAC address table on the QSW-8200 series switch. To maximize the use of the MAC address table, the QSW-8200 series switch uses the aging mechanism to update the MAC address table. For example, when the QSW-8200 series switch creates a dynamic entry, it starts the aging timer. If it does not receive packets from the MAC address in the entry during the aging time, the QSW-8200 series switch will delete the entry.

MAC address limit

MAC address limit is to limit the number of MAC addresses, avoid extending the searching time of forwarding entry caused by too large MAC address table and degrading the forwarding performance of the Ethernet switch, and it is effective to manage the MAC address table.

MAC address limit improves the speed of forwarding packets.

2.1.2 Preparing for configurations

Scenario

When you configure the MAC address table, configure static MAC address entries for the devices that are fixed in location and important. This prevents unauthorized users from accessing the network by forging a MAC address from other locations.

To prevent a device from accessing the network, configure its MAC address as a blackhole MAC address entry so that all packets with its MAC address as the destination or source MAC address will be discarded.

Configure the aging time of dynamic MAC addresses to avoid saving excessive MAC address entries in the MAC address table and running out of MAC address resources, and to achieve aging of dynamic MAC addresses.

Prerequisite

N/A

2.1.3 Default configurations of MAC address table

Default configurations of the MAC address table are as below.

Function	Default value
MAC address learning status	Enable
MAC address aging time	300s
MAC address learning limit	Unlimit
Global MAC address drift inhibition	Disable
Global MAC address drift alarm	Disable

2.1.4 Configuring static MAC address

Note

- Before configuring the static unicast MAC address, create a VLAN for it, activate the VLAN, and associate related interfaces with the VLAN.
- Before configuring the blackhole MAC address, create a VLAN for it, and activate the VLAN.

Configure static MAC addresses for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**mac-address-table static unicast** *mac-address* **vlan** *vlan-id* **port** *port-id*	Configure static unicast MAC address entries.
	Qtech(config)#**mac-address-table static multicast** *mac-address* **vlan** *vlan-id* **port-list** *port-list*	Configure the static unicast MAC address.
	Qtech(config)#**mac-address-table blackhole** *mac-address* **vlan** *vlan-id*	Configure blackhole MAC address entries.
3	Qtech(config)#**mac-address-table multicast filter** { **all** | **vlan** *vlan-list* }	(Optional) configure multicast filtering mode for the MAC address table.

2.1.5 Configuring dynamic MAC address

Configure dynamic MAC address for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**mac-address-table learning enable** { **port-list** *port-list* | **vlanlist** *vlan-list* }	Configure dynamic MAC address entry learning.
3	Qtech(config)#**mac-address-table aging-time** { **0** | *period* }	(Optional) configure the aging time of dynamic MAC address entries. The value 0 indicates no aging.
4	Qtech(config)#**interface port** *port-id* Qtech(config-port)#**mac-address-table threshold** *threshold-value*	Enter physical layer interface configuration mode. (Optional) configure dynamic MAC address limit on the interface.

2.1.6 Configuring drift control over MAC addresses

Configure drift control over MAC address for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**mac-address-table mac-move enable**	Enable global drift control over MAC addresses.
3	Qtech(config)#**mac-address-table trap enable**	Enable trap sending upon global drift control over MAC addresses.

2.1.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Qtech#show mac-address-table static [ port port-id | vlan vlan-id ]`	Show static unicast MAC address entries.
2	`Qtech#show mac-address-table multicast [ vlan vlan-id ] [ count ]`	Show Layer 2 multicast addresses or the number of existing multicast MAC addresses.
3	`Qtech#show mac-address-table blackhole`	Show blackhole MAC address entries.
4	`Qtech#show mac-address-table l2-address [ count ] [ vlan vlan-id | port port-id ]`	Show all Layer 2 unicast addresses and the current unicast MAC address limit.
5	`Qtech#show mac-address-table learning [ port port-id ]`	Show dynamic MAC address entry learning.
6	`Qtech#show mac-address-table threshold [ port-list port-list ]`	Show dynamic MAC address limit.
7	`Qtech#show mac aging-time`	Show the aging time of dynamic MAC address entries.

2.1.8 Maintenance

Maintain the QSW-8200 series switch as below.

Command	Description
`Qtech(config)#clear mac-address-table { all | blackhole | dynamic | static }`	Clear MAC address entries.
`Qtech(config)#search mac-address mac-address { all | dynamic | static } [ port port-id ] [ vlan vlan-id ]`	Search for a MAC address entry.

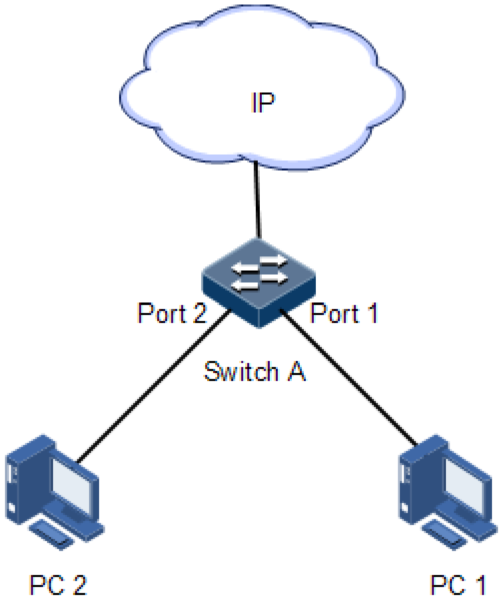
2.1.9 Example for configuring MAC address table

Networking requirements

As shown in Figure 2-1, PC 1 and PC 2 belong to VLAN 10. The MAC address of PC 1 is 001F.CE01.0105 while the MAC address of PC 2 is 001F.CE02.0207. PC 2 once used the MAC address of PC 1 to maliciously access the network. To prevent PC 2 from accessing the network without affecting other PCs to access the network from Port 2, configure the network as below.

- Set port 1 on Switch A with a static MAC address entry corresponding to the MAC address of PC 1, and disable dynamic MAC address learning.
- Set the MAC address of PC 2 as a blackhole MAC address entry, enable dynamic MAC address learning, and set the aging time to 400s.

Figure 2-1 MAC address table networking



Configuration steps

Step 1 Create VLAN 10, active it, and add interfaces into it.

```
Qtech#config
Qtech(config)#create vlan 10 active
Qtech(config)#interface port 1
Qtech(config-port)#switchport mode access
Qtech(config-port)#switchport access vlan 10
Qtech(config-port)#exit
Qtech(config)#interface port 2
Qtech(config-port)#switchport mode access
Qtech(config-port)#switchport access vlan 10
Qtech(config-port)#exit
```

Step 2 Configure a static unicast MAC address on Port 1, and disable dynamic MAC address learning.

```
Qtech(config)#mac-address-table static unicast 001F.CE01.0105 vlan 10
port 1
Qtech(config)#mac-address-table learning disable port-list 1
```

Step 3 Configure a blackhole MAC address for Port 2, enable dynamic MAC address learning, and set the aging time of dynamic MAC addresses to 400s.

```
Qtech(config)#mac-address-table blackhole 001F.CE02.0207 vlan 10
Qtech(config)#mac-address-table learning enable port-list 2
Qtech(config)#mac-address-table aging-time 400
```

Checking results

Use the **show mac-address-table l2-address port** *port-id* command to show configurations of the MAC address table.

```
Qtech#show mac-address-table l2-address port 2
Aging time: 400 seconds
Mac Address      Port        Vlan    Flags
-------------------------------------------------------
001F.CE01.0105     P1          10      static
001F.CE02.0207     --          10      blackhole
```

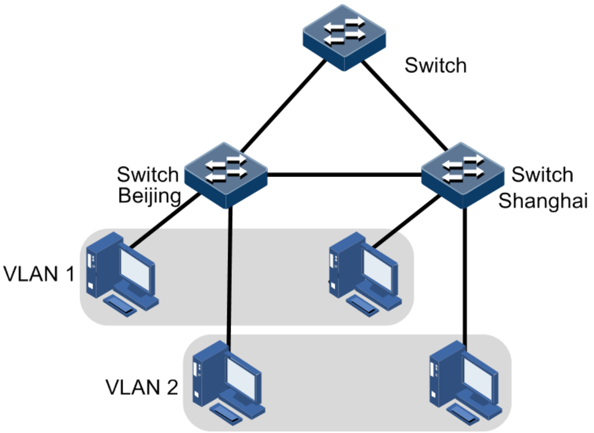
2.2 VLAN

2.2.1 Introduction

Overview

Virtual Local Area Network (VLAN) is a protocol to solve Ethernet broadcast and security problem. It is a Layer 2 isolation technique that partitions a LAN into different broadcast domains logically rather than physically, and then the different broadcast domains can work as virtual groups without any influence from one another. In terms of functions, VLAN has the same features as LAN, but members in one VLAN can access one another without restriction by physical location, as shown in Figure 2-2.

Figure 2-2 Partitioning VLANs



VLAN technique can partition a physical LAN into different broadcast domains logically. Hosts without intercommunication requirements can be isolated by VLAN, so VLAN partitioning improves network security, and reduces broadcast flow and broadcast storm.

The QSW-8200 series switch supports partitioning VLANs based on interface.

The QSW-8200 series switch complies with IEEE 802.1Q standard VLANs and supports 4094 concurrent VLANs.

Interface modes and packet forwarding

The QSW-8200 series switch has two interface modes: Access mode and Trunk mode.

Table 2-1 lists interfaces modes for processing packet.

Table 2-1 Interface modes and packet forwarding

Interface type	Processing ingress packets		Processing egress packets
	Untag packet	Tag packet	
Access	Add Access VLAN Tag into the packet.	• If VLAN ID of the packet is equal to Access VLAN ID, receive the packet. • If VLAN ID of the packet is not equal to Access VLAN ID, discard the packet.	• If the VLAN ID of the packet is equal to Access VLAN ID, remove Tag and send the packet. • If the packet VLAN ID is not included in the VLAN ID list allowed to pass by the interface, discard the packet.
Trunk	Add Native VLAN Tag into the packet.	• If the packet VLAN ID is included in the VLAN ID list allowed to pass by the interface, receive the packet. • If the packet VLAN ID is not included in the VLAN ID list allowed to pass by the interface, discard the packet.	• If the VLAN ID of the packet is equal to Native VLAN ID, remove Tag and send the packet. • If the VLAN ID of the packet is not equal to Native VLAN ID and the interface allows the packet to pass, keep the original Tag and send the packet.

Note

- By default, the default VLAN of the QSW-8200 series switch is VLAN 1.
- By default, the Access VLAN of the Access interface is VLAN 1, and the Native VLAN of the Trunk interface is VLAN 1.
- By default, VLAN 1 is in the list allowed by all interfaces. Use the **switchport access egress-allowed vlan** { { **all** | *vlan-list* } [**confirm**] | { **add** | **remove** } *vlan-list* } command to modify the VLAN list allowed to pass by the Access interface. Use the **switchport trunk allowed vlan** { { **all** | *vlan-list* } [**confirm**] | { **add** | **remove** } *vlan-list* } command to modify the VLAN list allowed to pass by the Trunk interface.

2.2.2 Preparing for configurations

Scenario

The main function of VLAN is to partition logic network segments. There are 2 typical application modes:

- One kind is that in a small LAN several VLANs are created on a device, the hosts that connect to the device are divided by VLAN. So hosts in the same VLAN can communicate, but hosts between different VLANs cannot communicate. For example, the financial department needs to be separated from other departments and they cannot access each other. Generally, the interface to connect host is in Access mode.
- The other kind is that in bigger LAN or enterprise network multiple devices connect to multiple hosts and the devices are cascaded, and data packets carry VLAN Tag for forwarding. The interfaces in the same VLAN on multiple devices can communicate, but the interfaces in different VLANs cannot communicate. This mode is used in enterprise that has many employees and needs a large number of hosts, in the same department but different position, the hosts in one department can access one another, so users have to partition VLANs on multiple devices. Layer 3 devices like router are required if users want to communicate among different VLAN. The cascaded interfaces among devices are set in Trunk mode.

When configuring the IP address for VLAN, you can associate a Layer 3 interface for it. Each Layer 3 interface corresponds to one IP address and one VLAN.

Prerequisite

N/A

2.2.3 Default configurations of VLAN

Default configurations of VLAN are as below.

Function	Default value
Create VLAN	VLAN 1
Active status of static VLAN	Suspend
Interface mode	Access
Access VLAN	VLAN 1

Function	Default value
Native VLAN of Trunk interface	VLAN 1
Permitted VLAN in Trunk mode	All VLANs
Permitted Untag VLAN in Trunk mode	VLAN 1
VLAN mapping table number	VLAN ID

2.2.4 Configuring VLAN attributes

Configure VLAN attributes for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**create vlan** *vlan-list* { **active** | **suspend** }	Create VLANs. The command can also be used to create VLANs in batches.
3	Qtech(config)#**vlan** v*lan-id*	Enter VLAN configuration mode.
4	Qtech(config-vlan)#**name** *vlan-name*	(Optional) configure VLAN name.
5	Qtech(config-vlan)#**state** { **active** | **suspend** }	Configure VLAN in active or suspend status.
6	Qtech(config-vlan)#**fid** *vlan-id*	Configure the VLAN mapping table number.

Note

- The VLAN created by the **vlan** *vlan-id* command is in suspend status, you need to use the **state active** command to activate the VLAN to make it take effect in the system.
- By default, there are two VLANs in system, the default VLAN (VLAN 1) and cluster VLAN (VLAN 2). All interfaces in Access mode belong to default VLAN. Both VLAN 1 and VLAN 2 cannot be created and deleted.
- By default, the default VLAN (VLAN 1) is called Default; cluster VLAN (VLAN 2) is called VLAN0002. Other VLAN is named as "VLAN+4-digit VLAN ID". For example, VLAN10 is named VLAN0010 by default, and VLAN4094 is named VLAN4094 by default.
- All configurations of VLAN do not take until the VLAN is activated. When VLAN status is Suspend, you cannot configure the VLAN, such as deleting/adding interface, setting VLAN name. The system will save the configurations. Once the VLAN is activated, the configurations will take effect in the system.

2.2.5 Configuring interface mode

Configure interface mode as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Qtech(config-port)#`**`switchport mode`** `{` **`access`** `|` **`trunk`** `}`	Configure the interface to Access or Trunk mode.

2.2.6 Configuring VLAN on Access interface

Configure VLANs on the Access interface for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.

3	`Qtech(config-port)#`**`switchport mode access`**
	`Qtech(config-port)#`**`switchport access vlan`** *`vlan-id`*
		Configure the interface in Access mode, and add the Access interface into the VLAN.

4	`Qtech(config-port)#`**`switchport access egress-allowed vlan`** `{` **`all`** `| [` **`add`** `|` **`remove`** `]` *`vlan-list`* `}`	(Optional) configure the VLAN allowed to pass by the Access interface.

Note

- The interface allows Access VLAN packets to pass regardless of configuration for VLAN allowed by the Access interface. The forwarded packets do not carry VLAN Tag.
- When setting Access VLAN, the system creates and activates VLAN automatically if you have not created and activated VLAN in advance.
- If you delete or suspend Access VLAN manually, the system will set the interface Access VLAN as default VLAN automatically.
- When configuring interface Access VLAN as non-default Access VLAN, default Access VLAN 1 is Access the egress interface allowed VLAN, you can delete Access VLAN 1 from allowed VLAN list of Access the egress interface by deleting this VLAN.
- If the configured Access VLAN is not default VLAN and there is no default VLAN in allowed VLAN list of Access interface, the interface does not permit default VLAN packets to pass.
- The allowed VLAN list of the Access interface is only effective to static VLANs, and ineffective to cluster VLANs, GVRP dynamic VLANs, etc.

2.2.7 Configuring VLAN on Trunk interface

Configure VLANs on the Trunk interface for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**switchport mode trunk**	Configure the interface in Trunk mode.
4	Qtech(config-port)#**switchport trunk native vlan** *vlan-id*	Configure interface Native VLAN.
5	Qtech(config-port)#**switchport trunk allowed vlan** { **all** | [**add** | **remove**] *vlan-list* }	(Optional) configure VLANs allowed to pass by the Trunk interface.
6	Qtech(config-port)#**switchport trunk untagged vlan** { **all** | [**add** | **remove**] *vlan-list* }	(Optional) configure VLANs from which the Trunk interface can remove Tag.

Note

- The interface allows Native VLAN packets to pass regardless of configuration on Trunk interface allowed VLAN list and Untagged VLAN list, the forwarded packets do not carry VLAN Tag.
- The system will create and activate the VLAN if no VLAN was created and activated in advance when setting Native VLAN.
- System set the interface Trunk Native VLAN as default VLAN if you have deleted or blocked Native VLAN manually.
- The interface allow incoming and outgoing VLAN packet allowed by the Trunk interface. If the VLAN is Trunk Untagged VLAN, the packets remove VLAN TAG at the egress interface, otherwise, do not modify the packets.
- If the configured Native VLAN is not default VLAN, and there is no default VLAN in Trunk interface allowed VLAN list, the interface will not allow default VLAN packets to pass.
- When setting Trunk Untagged VLAN list, system automatically adds all Untagged VLAN into Trunk allowed VLAN.
- Trunk allowed VLAN list and Trunk Untagged VLAN list are only effective to static VLAN, and ineffective for cluster VLAN, GVRP dynamic VLAN, etc.

2.2.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show vlan** [*vlan-list* | **static**]	Show VLAN configurations.

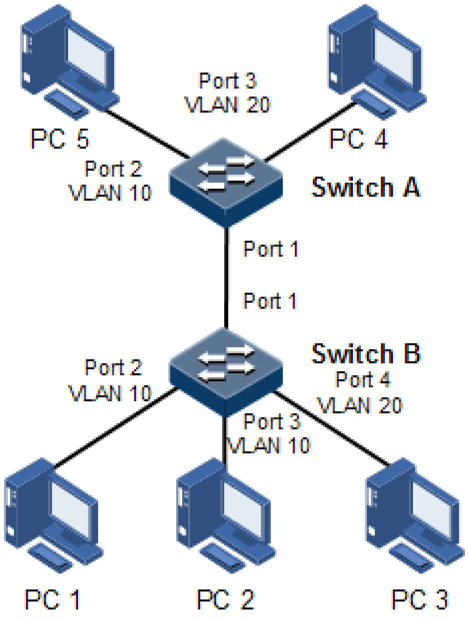
No.	Command	Description
2	Qtech#**show interface port-list** [*port-list*] **switchport**	Show VLAN configuration on the interface.

2.2.9 Configuring VLAN and interface protection

Networking requirements

As shown in Figure 2-3, PC 1, PC 2, and PC 5 belong to VLAN 10, PC 3 and PC 4 belong to VLAN 20; Switch A and Switch B are connected by Trunk interface; PC 3 and PC 4 cannot communicate because VLAN20 is not allowed to pass in the link; PC 1 and PC 2 under the same Switch B are enabled with interface protection function so that they cannot communicate with each other, but can respectively communicate with PC 5.

Figure 2-3 VLAN and interface protection networking



Configuration steps

Step 1 Create VLAN 10 and VLAN 20 on the two Switch devices respectively, and activate them.

Configure Switch A.

```
Qtech#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 10,20 active
```

Configure Switch B.

```
Qtech#hostname SwitchB
SwitchB#config
SwitchB(config)#create vlan 10,20 active
```

Step 2 Add port 2 and port 3 as Access mode on Switch B into VLAN 10, add port 4 as Access mode into VLAN 20, set port 1 to Trunk mode, and allow VLAN 10 to pass.

```
SwitchB(config)#interface port 2
SwitchB(config-port)#switchport mode access
SwitchB(config-port)#switchport access vlan 10
SwitchB(config-port)#exit
SwitchB(config)#interface port 3
SwitchB(config-port)#switchport mode access
SwitchB(config-port)#switchport access vlan 10
SwitchB(config-port)#exit
SwitchB(config)#interface port 4
SwitchB(config-port)#switchport mode access
SwitchB(config-port)#switchport access vlan 20
SwitchB(config-port)#exit
SwitchB(config)#interface port 1
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#switchport trunk allowed vlan 10 confirm
SwitchB(config-port)#exit
```

Step 3 Add port 2 as Access mode on Switch A into VLAN 10, add port 3 as Access mode into VLAN 20, set port 1 to Trunk mode, and allow VLAN 10 to pass.

```
SwitchA(config)#interface port 2
SwitchA(config-port)#switchport mode access
SwitchA(config-port)#switchport access vlan 10
SwitchA(config-port)#exit
SwitchA(config)#interface port 3
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport trunk native vlan 20
SwitchA(config-port)#exit
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport trunk allowed vlan 10 confirm
```

Step 4 Enable interface protection on port 2 and port 3 on Switch B.

```
SwitchB(config)#interface port 2
SwitchB(config-port)#switchport protect
SwitchB(config-port)#exit
SwitchB(config)#interface port 3
SwitchB(config-port)#switchport protect
```

Checking results

Use the **show vlan** command to show VLAN configurations.

Take Switch B for example.

```
SwitchB#show vlan
Switch Mode: --
VLAN Name          State   Status  Priority Member-Ports
--------------------------------------------------------------------------
------
1   Default        active  static  --       P 1-6
2   VLAN0002       active  other   --       P 1-28
10  VLAN0010       active  static  --       P 1,3-4
20  VLAN0020       active  static  --       P 5
```

Use the **show interface port** *port-id* **switchport** command to show configurations of the interface VLAN.

Take Switch B for example.

```
SwitchB#show interface port-list 2 switchport
Interface: port2
Reject frame type: none
Administrative Mode: access
Operational Mode: access
Access Mode VLAN: 10
Administrative Access Egress VLANs: 1
Operational Access Egress VLANs: 1,10
Trunk Native Mode VLAN: 1
Administrative Trunk Allowed VLANs: 1-4094
Operational Trunk Allowed VLANs: 1,10,20
Administrative Trunk Untagged VLANs: 1
Operational Trunk Untagged VLANs: 1
Vlan-mapping-miss Mode:Forwording
```

Use the **show switchport protect** command to show configurations of interface protection.

```
SwitchB#show switchport protect
Port     Protected State
--------------------------
  P1       enable
  P2       enable
  P3       enable
  P4       enable
  P5      disable
  P6      disable
  P7      disable
```

……

Check whether the Trunk interface permitting VLAN passing is correct by making PC 1 ping PC 5, PC 2 ping PC 5, and PC 3 ping PC 4.

- PC 1 can ping through PC 5, so VLAN 10 communication is normal.
- PC 2 can ping through PC 5, so VLAN 10 communication is normal.
- PC 3 fails to ping through PC 4, so VLAN 20 communication is abnormal.

Check whether interface protection is correct by making PC 1 ping PC 2.

PC 1 fails to ping through PC 2, so interface protection has taken effect.

2.3 Customer VLAN

2.3.1 Introduction

The customer VLAN is the service VLAN provided by the device. The unknown multicast and broadcast packets in the customer VLAN are directly forwarded without being processed. The unknown multicast and broadcast packets out of the customer VLAN are flooded to the CPU.

2.3.2 Configuring customer VLAN

Configure customer VLAN for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`customer-vlan`** *`vlan-list`*	Configure customer VLAN.

3	`Qtech(config)#`**`exit`**
	`Qtech#`**`show customer-vlan`**
		Show customer VLAN configurations.

2.4 QinQ

2.4.1 Introduction

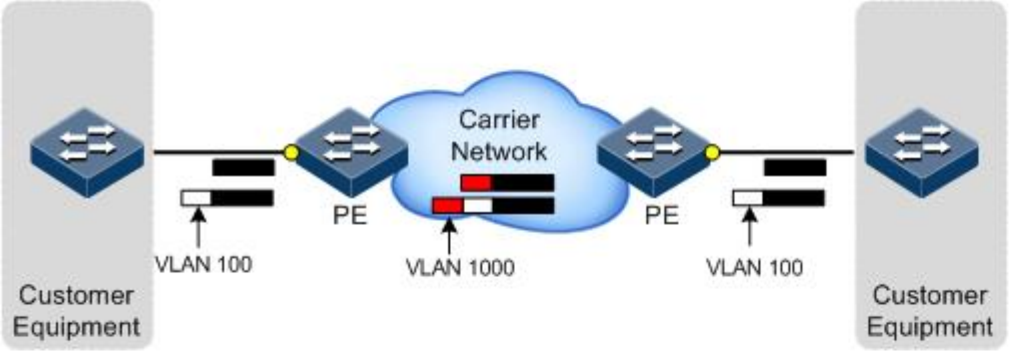
QinQ (also known as Stacked VLAN or Double VLAN) technique is an extension to 802.1Q defined in IEEE 802.1ad standard.

Basic QinQ

Basic QinQ is a simple Layer 2 VPN tunnel technique, which encapsulates outer VLAN Tag for user private network packets at carrier access end, then the packet takes double VLAN Tag to transmit through backbone network (public network) of the carrier. On the public network, packets are transmitted in accordance with outer VLAN Tag (namely the public network VLAN Tag), the user private network VALN Tag is transmitted as data in packets.

Figure 2-4 shows typical networking of basic QinQ. Wherein, the QSW-8200 series switch is the PE.

Figure 2-4 Principle of basic QinQ



Packets are transmitted from the user device to the PE, and the VLAN ID of packet tag is 100. Packet will be added with outer tag with VLAN 1000 when traversing from the PE device at the network side interface to the carrier network.

Packets with the VLAN 1000 outer Tag are transmitted to PE device on the other side by the carrier, and then the PE will remove the outer tag VLAN 1000 and send packets to the user device. Now the packets return to carrying only one tag VLAN 100.

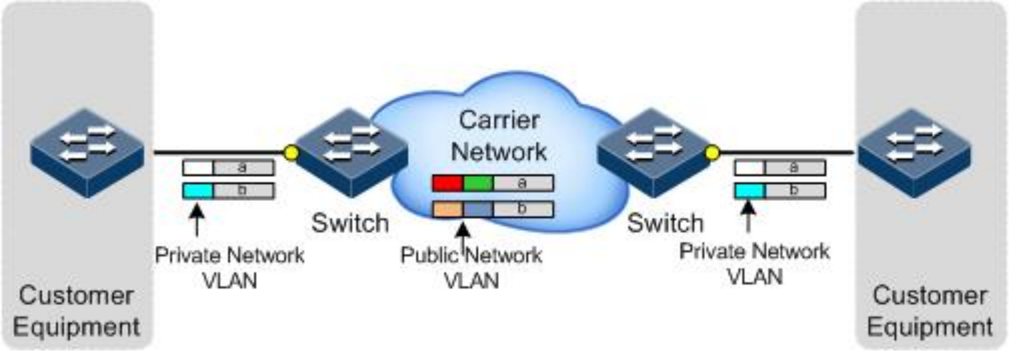
This technique can save public network VLAN ID resources. You can plan private network VLAN ID to avoid conflict with public network VLAN ID.

Selective QinQ

Selective QinQ is an enhancement to basic QinQ, which classifies flow according to user data features, then encapsulates different types flow into different outer VLAN Tags. This technique is realized by combination of interface and VLAN. Selective QinQ can perform different actions on different VLAN Tags received by one interface and add different outer VLAN IDs for different inner VLAN IDs. According to configured mapping rules for inner and outer Tags, you can encapsulate different outer Tags for different inner Tag packets.

As shown in Figure 2-5, selective QinQ makes structure of the carrier network more flexible. You can classify different terminal users on the access device interface by VLAN Tag and then, encapsulate different outer Tags for users in different classes. On the public network, you can configure QoS policy according to outer Tag and configure data transmission priority flexibly to make users in different classes receive corresponding services.

Figure 2-5 Principle of selective QinQ



TPID

Tag Protocol Identifier (TPID), a field in the VLAN Tag, indicates the protocol type of the VLAN Tag. IEEE 802.1Q defines its value as 0x8100.

The default TPID of packets of different vendors' devices may be different. To interconnect with other vendors' devices, set the TPID of the outer VLAN Tag of an interface to the TPID that can be identified by the connected device.

2.4.2 Preparing for configurations

Scenario

Basic QinQ configuration and selective QinQ configuration for the QSW-8200 series switch are based on different service requirements.

- Basic QinQ

With application of basic QinQ, you can add outer VLAN Tag to plan Private VLAN ID freely to make the user device data at both ends of carrier network transparently transmitted without conflicting with VLAN ID on the service provider network.

- Selective QinQ

Different from basic QinQ, outer VLAN Tag of selective QinQ can be selectable according to different services. There are multiple services and different private VLAN ID on the user network which are divided by adding different outer VLAN Tag for voice, video, and data services etc., then realizing different distributaries and inner and outer VLAN mapping for forwarding different services.

Prerequisite

- Connect interfaces.
- Configure physical parameters to make interfaces Up at the physical layer.
- Create VLANs.

2.4.3 Default configurations of QinQ

Default configurations of QinQ are as below.

Function	Default value
Outer VLAN Tag TPID	0x8100
Basic QinQ status	Disable
Selective QinQ status	Disable

2.4.4 Configuring basic QinQ

Configure basic QinQ on the ingress interface for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**switchport qinq dot1q-tunnel** [**default-cvlan** *vlan-id*]	Enable basic QinQ functions on the interface.
4	Qtech(config-port)#**switchport reject-frame** { **tagged** | **untagged** }	Configure the type of packets that are forbidden from being forwarded.

Note

- To use basic QinQ functions on an interface, configure its attributes first by setting it to the Access or Trunk interface and configuring the default VLAN.
- When basic QinQ is enabled on the interface, all packets are processed as Untagged packets. If you configure the Untagged packets to be discarded, Tagged packets are discarded as well.

2.4.5 Configuring selective QinQ

Configure selective QinQ on the ingress interface for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**switchport qinq dot1q-tunnel** [**default-cvlan** *vlan-id*]	Enable basic QinQ on the interface.
4	Qtech(config-port)#**switchport vlan-mapping cvlan** *custom-vlan-list* [**cos** *cos-value*] **add-outer** *outer-vlan-id* [**cos** *cos-value*] [**translate** *custom-vlan-id*]	Configure selective QinQ, add VLAN ID based on inner VLAN, and map the VLAN ID of inner VLAN.
	Qtech(config-port)#**switchport vlan-mapping cvlan** *custom-vlan-list* [**cos** *cos-value*] **add-outer** *outer-vlan-id* [**cos** *cos-value*] [**remove**]	Configure selective QinQ, add outer VLAN ID based on inner VLAN, and delete the inner VLAN.
	Qtech(config-port)#**switchport vlan-mapping ip-access-list** *ip-access-list* **add-outer** *outer-vlan-id* [**cos** *cos-value*]	Configure selection QinQ based on IP-ACL.

Step	Command	Description
	Qtech(config-port)# **switchport vlan-mapping mac-access-list** *mac-access-list* **add-outer** *outer-vlan-id* [**cos** *cos-value*]	Configure selection QinQ based on MAC-ACL.
	Qtech(config-port)#**switchport vlan-mapping cvlan untag add-outer** *outer-vlan-id* [**cos** *cos-value*]	Configure rules for adding outer VLAN Tag to Untag packets.
	Qtech(config-port)#**switchport vlan-mapping cvlan priority-tagged** [**cos** *cos-value*] **add-outer** *outer-vlan-id* [**cos** *cos-value*] [**translate** *custom-vlan-id* | **remove**]	Configure mapping rules for Tag VLAN of selective QinQ.
5	Qtech(config-port)#**switchport vlan-mapping-miss discard**	Configure the interface to discard packets that do not match selective QinQ or VLAN mapping rules.

Note

- Before configuring selective QinQ, configure basic QinQ.
- Do not configure *cos-value* and **translate** *custom-vlan-id* concurrently. Do not configure **cos** *cos-value* and **remove** concurrently.

2.4.6 Configuring network side interface to Trunk mode

Configure basic QinQ or selective QinQ on the network side interface for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**switchport mode trunk**	Configure interface trunk mode, and permit double Tag packet to pass.

2.4.7 Configuring TPID

Configure TPID on the network side interface for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.

Step	Command	Description
3	`Qtech(config-port)#mls double-tagging tpid tpid`	Configure the TPID of the outer VLAN Tag on the interface.

2.4.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Qtech#show switchport port port-list qinq`	Show configurations of basic QinQ and TPID.
2	`Qtech#show switchport port port-list vlan-mapping add-outer`	Show configurations of selective QinQ.
3	`Qtech#show switchport port-list port-list vlan-mapping acl add-outer`	Show configurations of selective QinQ based on ACL.

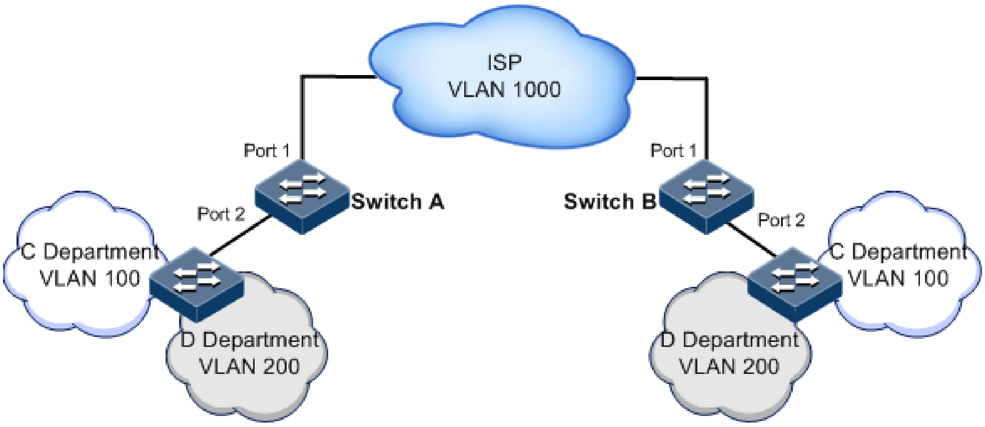
2.4.9 Example for configuring basic QinQ

Networking requirements

As shown in Figure 2-6, Switch A and Switch B are connected to VLAN 100 and VLAN 200 respectively. Department C and Department D need to communicate through the carrier network, but their networks are isolated from each other. The carrier TPID is 9100.

Configure basic QinQ on Switch A and Switch B to implement normal communication through the carrier's network.

Figure 2-6 Basic QinQ networking



Configuration steps

Configure Switch A and Switch B.

Configuration steps for switch A and Switch B are the same. Take Switch A for example.

Step 1 Create VLAN 100, VLAN 200, and VLAN 1000, and activate them.

```
Qtech#config
Qtech(config)#create vlan 100,200,1000 active
Qtech(config)#interface port 1
Qtech(config-port)#switchport mode trunk
Qtech(config-port)#switchport trunk allowed vlan 1000
Qtech(config-port)#mls double-tagging tpid 9100
Qtech(config-port)#exit
```

Step 2 Enable basic QinQ.

```
Qtech(config)#interface port 2
Qtech(config-port)#switchport mode trunk
Qtech(config-port)#switchport trunk native vlan 1000
Qtech(config-port)#switchport qinq dot1q-tunnel
Qtech(config-port)#exit
```

Checking results

Use the **show switchport qinq** command to show QinQ configurations.

```
Qtech#show switchport port-list 1 qinq
Interface QinQ Status  Outer-TPID Default-CVlan
--------------------------------------------------------
p1    Disable      0x9100     -
Qtech#show switchport port-list 2 qinq
Interface QinQ Status  Outer-TPID Default-CVlan
--------------------------------------------------------
p2    Enable      0x8100     -
```

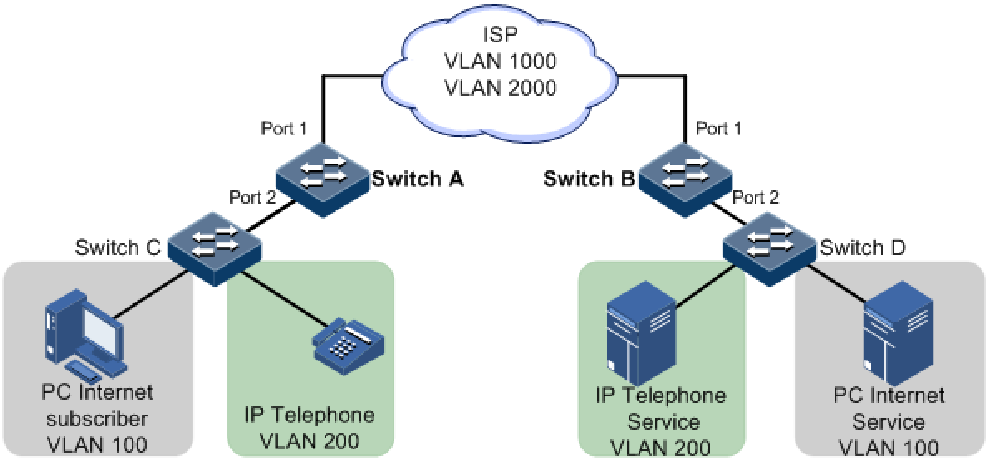
2.4.10 Example for configuring selective QinQ

Networking requirements

As shown in Figure 2-7, the carrier network carries common PC Internet service and IP phone service; PC Internet service is assigned to VLAN 1000; IP phone service is assigned to VLAN 2000. Configure Switch A and Switch B as below to make client and server communicate through carrier network:

- Configure selective QinQ on Switch A and Switch B.
- Add outer Tag VLAN 1000 to the VLAN 100 assigned to Internet service by the PC.
- Add outer Tag 2000 for VLAN 200 for IP phone service.
- The carrier TPID is 9100.

Figure 2-7 Selective QinQ networking



Configuration steps

Configure Switch A and Switch B.

Configuration steps for Switch A and Switch B are the same. Take Switch A for example.

Step 1 Create and activate VLAN 100, VLAN 200, VLAN 1000, and VLAN 2000. The TPID is 9100.

```
Qtech#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 100,200,1000,2000 active
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport trunk allowed vlan 1000,2000
SwitchA(config-port)#mls double-tagging tpid 9100
SwitchA(config-port)#exit
```

Step 2 Enable selective QinQ on port 2.

```
SwitchA(config)#interface port 2
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport qinq dot1q-tunnel
SwitchA(config-port)#switchport vlan-mapping cvlan 100 add-outer 1000
SwitchA(config-port)#switchport vlan-mapping cvlan 200 add-outer 2000
SwitchA(config-port)#exit
```

Checking results

Use the **show switchport port-list** *port-list* **vlan-mapping add-outer** command to show configurations of selective QinQ.

Take Switch A for example.

```
SwitchA#show switchport port-list 2 vlan-mapping add-outer
Based inner VLAN flexible QinQ mapping rule:
Interface CVLAN   Add-SVlan    Cos   CVlan-Action Translate-CVlan Hardware
-----------------------------------------------------------------------
p2    100     1000        0     Reserve      -             Yes
p2    200     2000        0     Reserve      -             Yes
```

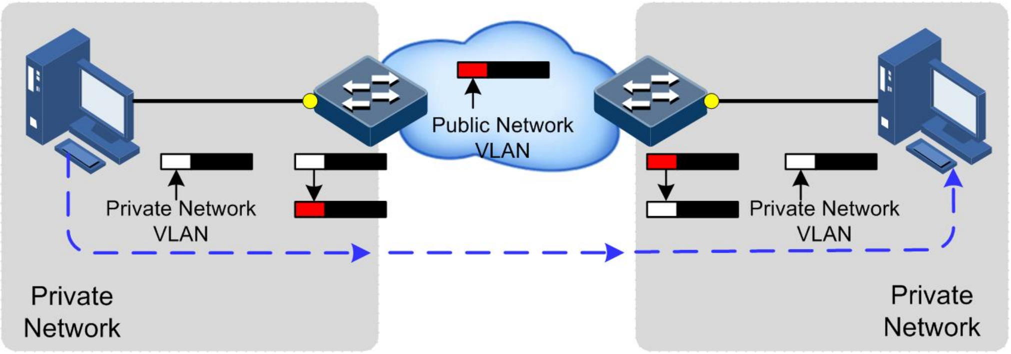
2.5 VLAN mapping

2.5.1 Introduction

VLAN mapping is used to replace the private VLAN Tag of Ethernet packets with carrier's VLAN Tag, making packets transmitted according to carrier's VLAN forwarding rules. When packets are sent to the peer private network from the ISP network, the VLAN Tag is restored to the original private VLAN Tag according to the same VLAN forwarding rules. Therefore packets are correctly sent to the destination.

Figure 2-8 shows the principle of VLAN mapping.

Figure 2-8 Principle of VLAN mapping



After receiving a VLAN Tag contained in a user private network packet, the QSW-8200 series switch matches VLAN Tag of the user private network packet according to configured VLAN mapping rules. If successful, it replaces the VLAN Tag according to configured VLAN mapping rules. By supporting 1: 1 VLAN mapping, the QSW-8200 series switch replaces the VLAN Tag carried by a packet from a specified VLAN with the new VLAN Tag.

Different from QinQ, VLAN mapping does not encapsulate packets with multiple layers of VLAN Tags, but needs to modify VLAN Tag so that packets are transmitted according to the carrier's VLAN forwarding rule.

2.5.2 Preparing for configurations

Scenario

Different from QinQ, VLAN mapping is to change the VLAN Tag without encapsulating multilayer VLAN Tag so that packets are transmitted according to the ISP's VLAN mapping rules. VLAN mapping does not increase the frame length of the original packet. It can be used in the following scenarios:

- A user service needs to be mapped to a carrier's VLAN ID.
- Multiple user services need to be mapped to a carrier's VLAN ID.

Prerequisite

- Connect interfaces.
- Configure physical parameters to make interfaces Up at the physical layer.
- Create VLANs.

2.5.3 Configuring VLAN mapping

Configure VLAN mapping for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**switchport vlan-mapping outer** *outer-vlan-id* **translate** *outer-new-vlan-id* [**cos** *cos-value*]	(Optional) configure outer-Tag-based VLAN mapping rule to translate outer VLAN only.
	Qtech(config-port)#**switchport vlan-mapping outer** *outer-vlan-id* **inner** *inner-vlan-id* **translate** *outer-new-vlan-id inner-new-vlan-id* [**cos** *cos-value*]	(Optional) configure dual-Tag-based VLAN mapping; namely, configure both outer-Tag-based and inner-Tag-based VLAN mapping. Configure both outer VLAN mapping and inner VLAN mapping.

2.5.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show switchport port-list** *port-list* **vlan-mapping translate**	Show VLAN mapping rules of the interface.

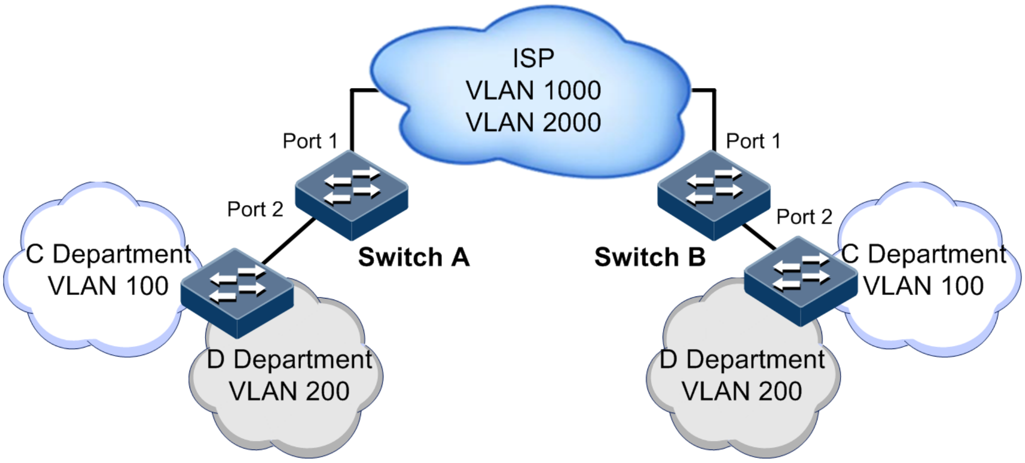
2.5.5 Example for configuring VLAN mapping based on single Tag

Scenario

As shown in Figure 2-9, Switch A and Switch B are connected to VLAN 100 and VLAN 200 respectively. Department C and Department D need to communicate through the carrier's network, but their networks are isolated from each other.

Between Switch A and Switch, 1: 1 VLAN mapping is configured to implement normal communication inside the department.

Figure 2-9 VLAN mapping networking



Configuration steps

Configure Switch A and Switch B.

Configuration steps for Switch A and Switch B are the same. Take Switch A for example.

Step 1 Create VLANs 100, 200, 1000, and 2000, and activate them.

```
Qtech#config
Qtech(config)#create vlan 100,200,1000,2000 active
```

Step 2 Set port 1 to Trunk mode, allowing VLAN 1000 and VLAN 2000 packets to pass.

```
Qtech(config)#interface port 1
Qtech(config-port)#switchport mode trunk
Qtech(config-port)#switchport trunk allowed vlan 1000,2000 confirm
Qtech(config-port)#exit
```

Step 3 Set port 2 to Trunk mode. Enable VLAN mapping.

```
Qtech(config)#interface port 2
Qtech(config-port)#switchport mode trunk
Qtech(config-port)#switchport vlan-mapping outer 100 translate 1000
Qtech(config-port)#switchport vlan-mapping outer 200 translate 2000
Qtech(config-port)#exit
```

Checking results

Use the **show switchport port-list** *port-list* **vlan-mapping translate** command to show configurations of VLAN mapping.

```
Qtech#show switchport port-list 2 vlan-mapping translate
        Original   Original   New      New
Interface Outer VLAN Inner VLAN Outer-VID Inner-VID Hardware
----------------------------------------------------------------------
P2    100       -        1000     -       Yes
P2    200       -        2000     -       Yes
```

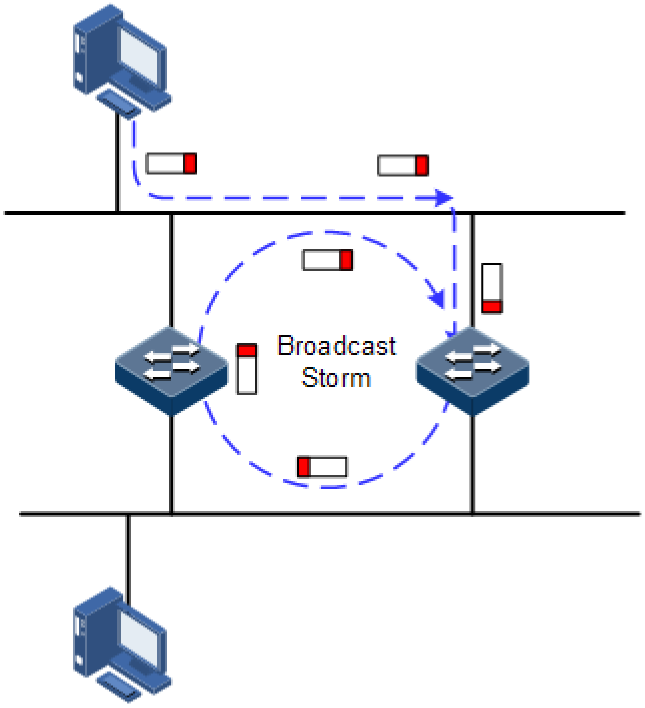
2.6 STP

2.6.1 Introduction

STP

With the increasing complexity of network structure and growing number of switches on the network, the Ethernet network loops become the most prominent problem. Because of the packet broadcast mechanism, a loop causes the network to generate storms, exhaust network resources, and have serious impact to forwarding normal data. The network storm caused by the loop is shown in Figure 2-10.

Figure 2-10 Network storm due to loop

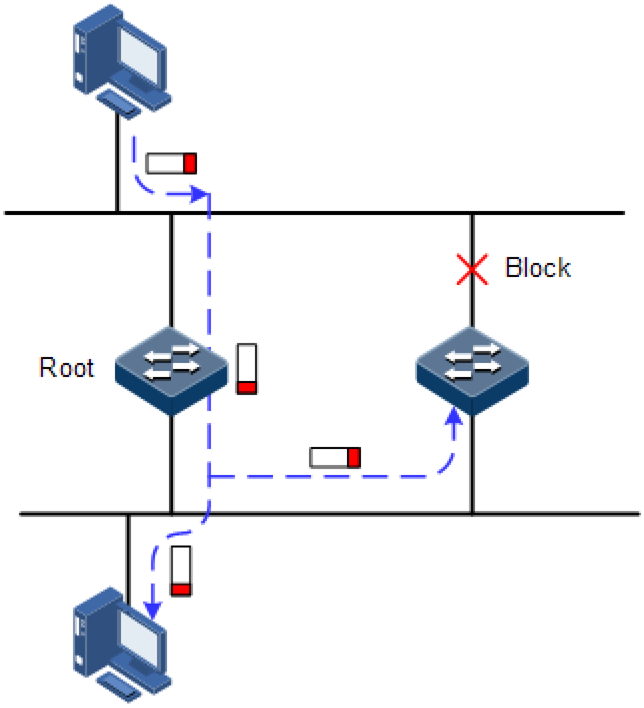


Spanning Tree Protocol (STP) is compliant to IEEE 802.1d standard and used to remove data physical loop in data link layer in the LAN.

The QSW-8200 series switch running STP can process Bridge Protocol Data Unit (BPDU) with each other for the election of root switch and selection of root port and designated port. It also can block loop interface on the QSW-8200 series switch logically according to the selection results, and finally trims the loop network structure to tree network structure without loop which takes an QSW-8200 series switch as root. This prevents the continuous proliferation and limitless circulation of packet on the loop network from causing broadcast storms and avoids declining packet processing capacity caused by receiving the same packets repeatedly.

Figure 2-11 shows loop networking running STP.

Figure 2-11 Loop networking with STP



Although STP can eliminate loop network and prevent broadcast storm well, its shortcomings are still gradually exposed with thorough application and development of network technology.

The major disadvantage of STP is the slow convergent speed.

2.6.2 Preparing for configurations

Networking situation

In a big LAN, multiple devices are concatenated for accessing each other among hosts. They need to be enabled with STP to avoid loop among them, MAC address learning fault, and broadcast storm and network crash caused by quick copy and transmission of data frames. STP calculation can block one interface in a broken loop and ensure there is only one path for the data flow to be transmitted to the destination host t, which is also the best path.

Preconditions

Configure interface physical parameters to make it Up.

2.6.3 Default configurations of STP

Default configurations of STP are as below.

Function	Default value
Global STP status	Disable
Interface STP status	Enable
STP priority of device	32768
STP priority of interface	128
Interface path cost	0
max-age timer	20s
hello-time timer	2s
forward-delay timer	15s

2.6.4 Enabling STP

Configure STP for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`spanning-tree mode stp`**	Configure the spanning tree mode to STP.
3	`Qtech(config)#`**`spanning-tree enable`**	Enable STP.

2.6.5 Configuring STP parameters

Configure STP parameters for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`spanning-tree priority`** *`priority-value`*	(Optional) configure device priority.
3	`Qtech(config)#`**`spanning-tree root { primary | secondary }`**	(Optional) configure the QSW-8200 series switch as the root or backup device.

4	`Qtech(config)#`**`interface port`** *`port-id`*
	`Qtech(config-port)#`**`spanning-tree priority`** *`priority-value`*
	`Qtech(config-port)#`**`exit`**
		(Optional) configure device interface priority.

Step	Command	Description
5	`Qtech(config)#spanning-tree hello-time value`	(Optional) configure Hello Time.
6	`Qtech(config)#spanning-tree transit-limit value`	(Optional) configure maximum transmission rate of interface.
7	`Qtech(config)#spanning-tree forward-delay value`	(Optional) configure forward delay.
8	`Qtech(config)#spanning-tree max-age value`	(Optional) configure maximum age.

2.6.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Qtech#show spanning-tree`	Show basic configurations of STP.
2	`Qtech#show spanning-tree port-list port-list`	Show STP configurations on the interface.

2.6.7 Maintenance

Maintain the QSW-8200 series switch as below.

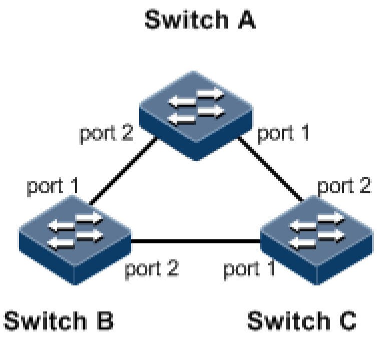
Command	Description
`Qtech(config-port)#spanning-tree clear statistics`	Clear statistics of interface spanning tree.

2.6.8 Example for configuring STP

Networking requirements

As shown in Figure 2-12, Switch A, Switch B, and Switch C forms a ring network, so the loopback problem must be solved in the situation of a physical ring. Enable STP on them, set the priority of Switch A to 0, and path cost from Switch B to Switch A to 10.

Figure 2-12 STP networking



Configuration steps

Step 1 Enable STP on Switch A, Switch B, and Switch C.

Configure Switch A.

```
Qtech#hostname SwitchA
SwitchA#config
SwitchA(config)#spanning-tree enable
SwitchA(config)#spanning-tree mode stp
```

Configure Switch B.

```
Qtech#hostname SwitchB
SwitchB#config
SwitchB(config)#spanning-tree enable
SwitchB(config)#spanning-tree mode stp
```

Configure Switch C.

```
Qtech#hostname SwitchC
SwitchC#config
SwitchC(config)#spanning-tree enable
SwitchC(config)#spanning-tree mode stp
```

Step 2 Configure interface mode on three switches.

Configure Switch A.

```
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#exit
SwitchA(config)#interface port 2
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#exit
```

Configure Switch B.

```
SwitchB(config)#interface port 1
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#exit
SwitchB(config)#interface port 2
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#exit
```

Configure Switch C.

```
SwitchC(config)#interface port 1
SwitchC(config-port)#switchport mode trunk
SwitchC(config-port)#exit
SwitchC(config)#interface port 2
SwitchC(config-port)#switchport mode trunk
SwitchC(config-port)#exit
```

Step 3 Configure priority of spanning tree and interface path cost.

Configure Switch A.

```
SwitchA(config)#spanning-tree priority 0
SwitchA(config)#interface port 2
SwitchA(config-port)#spanning-tree inter-path-cost 10
```

Configure Switch B.

```
SwitchB(config)#interface port 1
SwitchB(config-port)#spanning-tree inter-path-cost 10
```

Checking results

Use the **show spanning-tree** command to show bridge status.

- Switch A

```
SwitchA#show spanning-tree
Qtech#show spanning-tree
MSTP Admin State: Enable
Protocol Mode: STP
```

```
BridgeId:    Mac 001F.CE7B.C557  Priority 0
Root:       Mac 001F.CE7B.C557  Priority 0   RootCost 0
Operational:  HelloTime 2, ForwardDelay 15, MaxAge 20
Configured:   HelloTime 2, ForwardDelay 15, MaxAge 20 TransmitLimit 3
```

- Switch B

```
Qtech#show spanning-tree
MSTP Admin State: Enable
Protocol Mode: STP
BridgeId:    Mac 001F.CE83.ABD1  Priority 32768
Root:       Mac 001F.CE7B.C557  Priority 0   RootCost 10
Operational:  HelloTime 2, ForwardDelay 15, MaxAge 20
Configured:   HelloTime 2, ForwardDelay 15, MaxAge 20 TransmitLimit 3
```

- Switch C

```
Qtech#show spanning-tree
MSTP Admin State: Enable
Protocol Mode: STP
BridgeId:    Mac 001F.CE83.ABD5  Priority 32768
Root:       Mac 001F.CE7B.C557  Priority 0   RootCost 200000
Operational:  HelloTime 2, ForwardDelay 15, MaxAge 20
Configured:   HelloTime 2, ForwardDelay 15, MaxAge 20 TransmitLimit 3
```

Use the **show spanning-tree port-list** *port-list* command to show interface status.

- Switch A

```
Qtech#show spanning-tree port-list 1,2
Port ID:1
PortEnable: admin: enable       oper: enable
Rootguard:  disable
Loopguard:  disable
ExternPathCost:10
Partner MSTP Mode: stp
Bpdus send:   279  (TCN<0>   Config<279>  RST<0>  MST<0>)
Bpdus received:13  (TCN<13>   Config<0>  RST<0>  MST<0>)
State:forwarding  Role:designated     Priority:128   Cost: 200000
Root:       Mac 001F.CE7B.C557  Priority 0   RootCost 0
DesignatedBridge: Mac 001F.CE7B.C557  Priority 0   DesignatedPort 32777

Port ID:2
PortEnable: admin: enable       oper: enable
Rootguard:  disable
Loopguard:  disable
ExternPathCost:200000
Partner MSTP Mode: stp
```

```
Bpdus send:   279  (TCN<0>   Config<279>  RST<0>  MST<0>)
Bpdus received:6  (TCN<6>   Config<0>  RST<0>  MST<0>)
State:forwarding  Role:designated     Priority:128   Cost: 200000
Root:       Mac 001F.CE7B.C557  Priority 0   RootCost 0
DesignatedBridge: Mac 001F.CE7B.C557  Priority 0   DesignatedPort 32778
```

- Switch B

```
Qtech#show spanning-tree port-list 1,2
Port ID:1
PortEnable: admin: enable       oper: enable
Rootguard:  disable
Loopguard:  disable
ExternPathCost:200000
Partner MSTP Mode: stp
Bpdus send:   357  (TCN<0>   Config<357>  RST<0>  MST<0>)
Bpdus received:13  (TCN<12>   Config<1>  RST<0>  MST<0>)
State:forwarding  Role:designated     Priority:128   Cost: 200000
Root:       Mac 001F.CE7B.C557  Priority 0   RootCost 10
DesignatedBridge: Mac 001F.CE83.ABD1  Priority 32768   DesignatedPort
32777

Port ID:2
PortEnable: admin: enable       oper: enable
Rootguard:  disable
Loopguard:  disable
ExternPathCost:10
Partner MSTP Mode: stp
Bpdus send:   36  (TCN<13>   Config<23>  RST<0>  MST<0>)
Bpdus received:335  (TCN<0>   Config<335>  RST<0>  MST<0>)
State:forwarding  Role:root     Priority:128   Cost: 10
Root:       Mac 001F.CE7B.C557  Priority 0   RootCost 10
DesignatedBridge: Mac 001F.CE7B.C557  Priority 0   DesignatedPort 32777
```

- Switch C

```
Qtech#show spanning-tree port-list 1,2
Port ID:1
PortEnable: admin: enable       oper: enable
Rootguard:  disable
Loopguard:  disable
ExternPathCost:200000
Partner MSTP Mode: stp
Bpdus send:   22  (TCN<12>   Config<10>  RST<0>  MST<0>)
Bpdus received:390  (TCN<0>   Config<390>  RST<0>  MST<0>)
State:blocking  Role:non-designated     Priority:128   Cost: 200000
Root:       Mac 001F.CE7B.C557  Priority 0   RootCost 200000
DesignatedBridge: Mac 001F.CE83.ABD1  Priority 32768   DesignatedPort
32777
```

```
Port ID:2
PortEnable: admin: enable       oper: enable
Rootguard:  disable
Loopguard:  disable
ExternPathCost:200000
Partner MSTP Mode: stp
Bpdus send:   38  (TCN<6>   Config<32>  RST<0>  MST<0>)
Bpdus received:368  (TCN<0>   Config<368>  RST<0>  MST<0>)
State:forwarding  Role:root     Priority:128   Cost: 200000
Root:       Mac 001F.CE7B.C557  Priority 0   RootCost 200000
DesignatedBridge: Mac 001F.CE7B.C557  Priority 0   DesignatedPort 32778
```

2.7 RSTP/MSTP

2.7.1 Introduction

RSTP

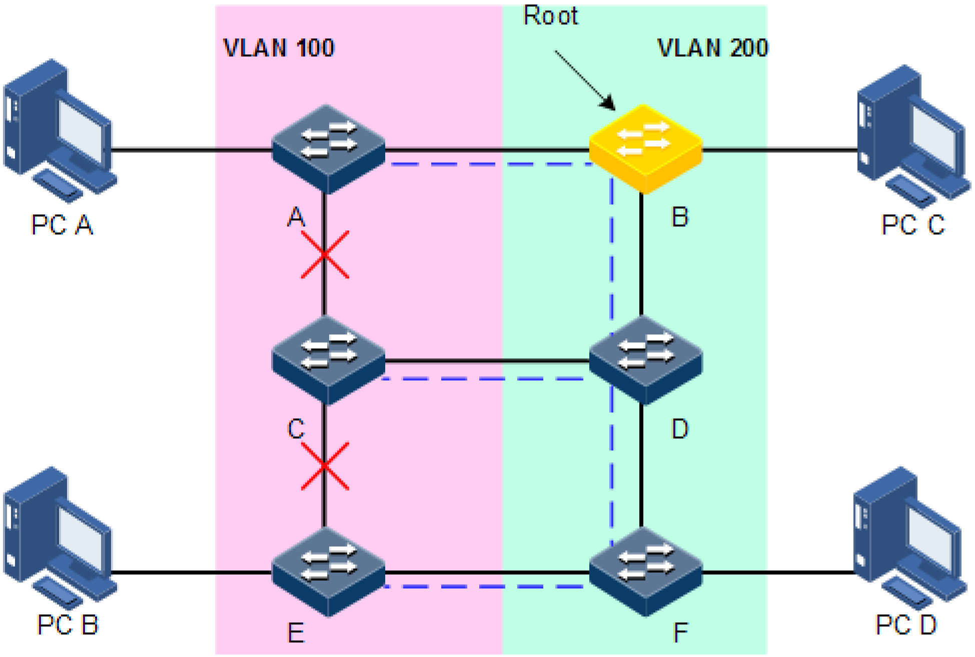
For improving the slow convergent speed of STP, IEEE 802.1w establishes Rapid Spanning Tree Protocol (RSTP), which increases the mechanism to change interface blocking state to forwarding state, speed up the topology convergence rate.

The purpose of STP/RSTP is to simplify a bridge connection LAN to a unitary spanning tree in logical topology and to avoid broadcast storm.

The disadvantages of STP/RSTP are exposed with the rapid development of VLAN technology. The unitary spanning tree simplified from STP/RSTP leads to the following problems:

- The whole switching network has only one spanning tree, which will lead to longer convergence time on a larger network.
- After a link is blocked, it does not carry traffic any more, causing waste of bandwidth.
- Packet of partial VLAN cannot be forwarded when network structure is unsymmetrical. As shown in Figure 2-13, Switch B is the root switch; RSTP blocks the link between Switch A and Switch C logically and makes that the VLAN 100 packet cannot be transmitted and Switch A and Switch C cannot communicate.

Figure 2-13 VLAN packet forward failure due to RSTP



MSTP

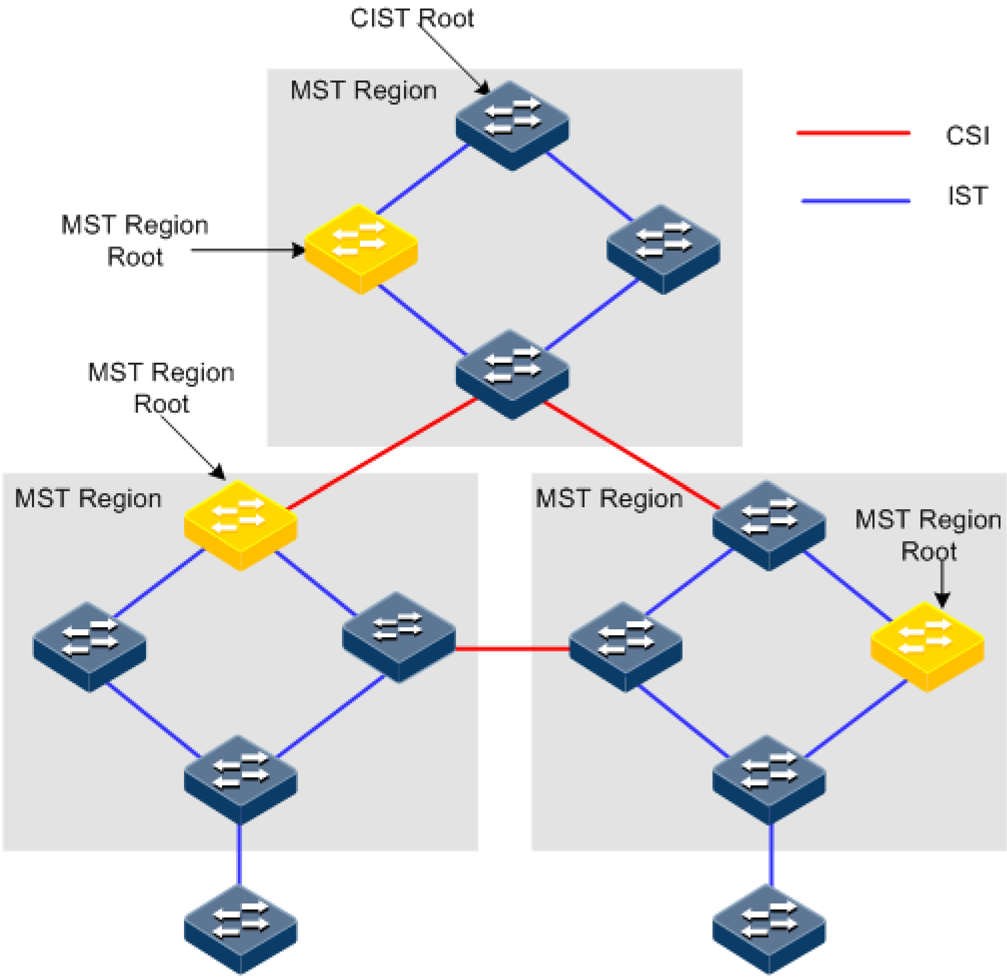
Multiple Spanning Tree Protocol (MSTP) is defined by IEEE 802.1s. Recovering the disadvantages of STP and RSTP, the MSTP realizes fast convergence and distributes different VLAN flows following their own paths to provide an excellent load sharing mechanism.

MSTP divides a switching network into multiple domains, called MST domain. Each MST domain contains several spanning trees but the trees are independent from each other. Each spanning tree is called a Multiple Spanning Tree Instance (MSTI).

MSTP protocol introduces Common Spanning Tree (CST) and Internal Spanning Tree (IST) concepts. CST refers to taking MST domain as a whole to calculate and generating a spanning tree. IST refers to generating spanning tree in internal MST domain.

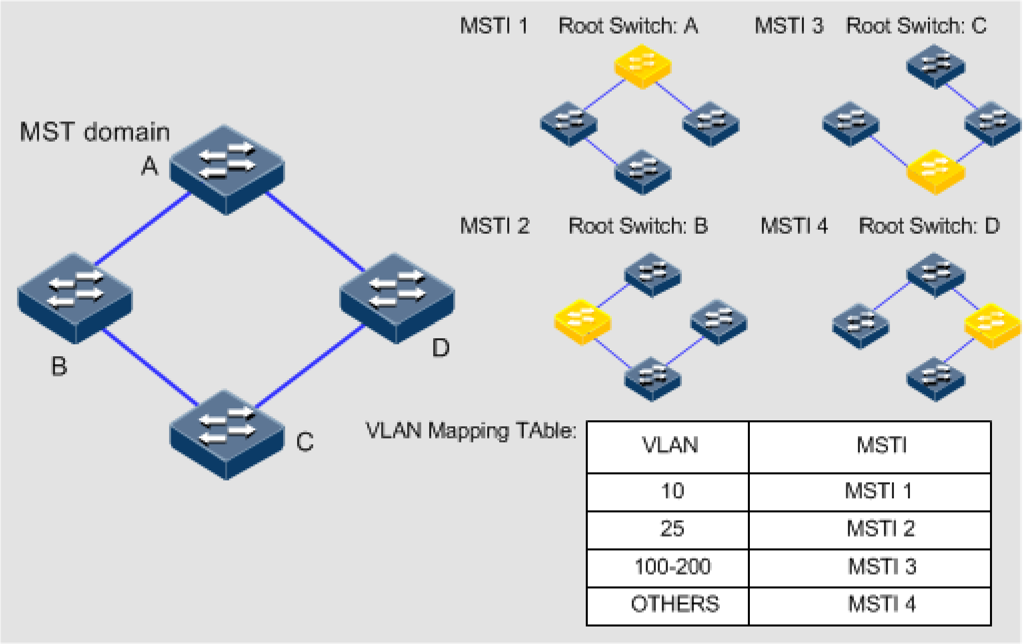
Compared with STP and RSTP, MSTP also introduces a CIST root and MST region root. The CIST root is a global concept; all switches running STP/RSTP/MSTP can have only one CIST Root. The MST region root is a local concept, which is relative to an instance in a domain. As shown in Figure 2-14, all connected devices only have one total root, and the number of domain root contained in each domain is associated with the number of instances.

Figure 2-14 Basic concepts of MSTI network



There can be different MSTIs in each MST domain, which associates VLAN and MSTI by setting VLAN mapping table (table for mapping VLAN and MSTI). The MSTI concepts are shown in Figure 2-15.

Figure 2-15 MSTI concepts



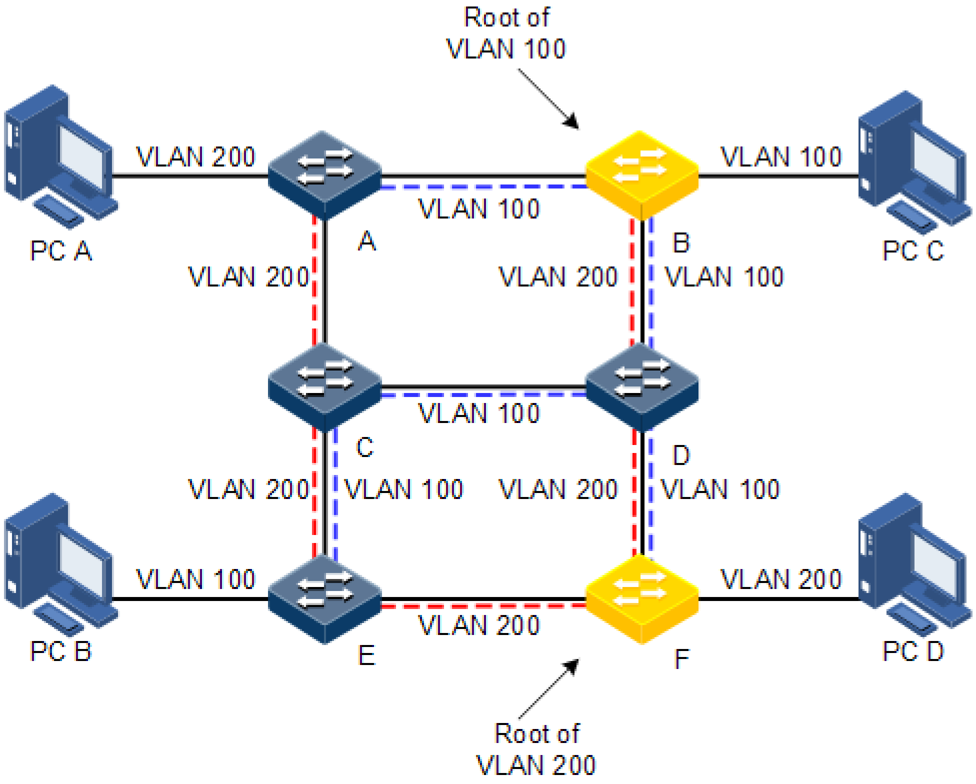
VLAN	MSTI
10	MSTI 1
25	MSTI 2
100-200	MSTI 3
OTHERS	MSTI 4

Note

Each VLAN can map to one MSTI; that is to say, data of one VLAN can only be transmitted in one MSTI while one MSTI may correspond to several VLANs.

Compared with the previous STP and RSTP, MSTP has obvious advantages, including cognitive ability of VLAN, load balance sharing ability, similar RSTP port status switching ability as well as binding multiple VLANs to one MSTI to reduce resource occupancy rate. In addition, MSTP running devices on the network are also compatible with the devices running STP and RSTP.

Figure 2-16 Networking of multiple spanning trees instances in MST domain



Applying MSTP in the network as Figure 3-10 above, after calculation, there are two spanning trees generated at last (two MSTIs):

- MSTI 1 takes Switch B as the root switch, forwarding packets of VLAN 100.
- MSTI 2 takes Switch F as the root switch, forwarding packets of VLAN 200.

In this way, all VLANs can communicate internally, different VLAN packets are forwarded in different paths to share load.

2.7.2 Preparing for configurations

Scenario

In big LAN or residential region aggregation, the aggregation devices make up a ring for link backup, at the same time avoid loop and realize service load sharing. MSTP can select different and unique forwarding path for each one or a group of VLANs.

Prerequisite

Configure interface physical parameters to make it Up.

2.7.3 Default configurations of MSTP

Default configurations of MSTP are as below.

Function	Default value
Global MSTP status	Disable
Interface MSTP status	Enable
Maximum number of hops for MST domain	20
MSTP priority of device	32768
MSTP priority of interface	128
Path cost of interface	0
Maximum number of packets sent within each Hello time	3
Max Age timer	20s
Hello Time timer	2s
Forward Delay timer	15s
Revision level of MST domain	0

2.7.4 Enabling MSTP

Configure MSTP for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`spanning-tree mode mstp`**	Configure the spanning tree mode to MSTP.
3	`Qtech(config)#`**`spanning-tree enable`**	Enable global STP.

2.7.5 Configuring MST domain and its maximum number of hops

You can set domain information about the QSW-8200 series switch when it is running in MSTP mode. The device MST domain is decided by domain name, VLAN mapping table and configuration of MSTP revision level. You can set current device in a specific MST domain through following configuration.

MST domain scale is restricted by the maximum number of hops. Starting from the root bridge of spanning tree in the domain, the configuration message (BPDU) reduces 1 hop count once it is forwarded passing a device; the QSW-8200 series switch discards the configuration message whose number of hops is 0. The device exceeding the maximum number of hops cannot join spanning tree calculation and then restrict MST domain scale.

Configure MSTP domain and its maximum number of hops for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**spanning-tree region-configuration**	Enter MST domain configuration mode.
3	Qtech(config-region)#**name** *name*	Configure MST domain name.
4	Qtech(config-region)#**revision-level** *level-value*	Set revision level for MST domain.
5	Qtech(config-region)#**instance** *instance-id* **vlan** *vlan-list* Qtech(config-region)#**exit**	Set mapping from MST domain VLAN to instance.
6	Qtech(config)#**spanning-tree max-hops** *hops-value*	Configure the maximum number of hops for MST domain.

Note

Only when the configured device is the domain root can the configured maximum number of hops be used as the maximum number of hops for MST domain; other non-domain root cannot be configured this item.

2.7.6 Configuring root bridge/backup bridge

Two methods for MSTP root selection are as below:

- To configure device priority and calculated by STP to confirm STP root bridge or backup bridge
- To assign MSTP root directly by a command

When the root bridge has a fault or powered off, the backup bridge can replace of the root bridge of related instance. In this case, if a new root bridge is assigned, the backup bridge will not become the root bridge. If several backup bridges for a spanning tree are configured, once the root bridge stops working, MSTP will choose the backup root with the smallest MAC address as the new root bridge.

Caution

We recommend not modifying the priority of any device on the network if you directly assign the root bridge; otherwise, the assigned root bridge or backup bridge may be invalid.

Configure root bridge or backup bridge for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**spanning-tree** [**instance** *instance-id*] **root** { **primary** | **secondary** }	Set the QSW-8200 series switch as root bridge or backup bridge for a STP instance.

Note

- You can confirm the effective instance of the root bridge or backup bridge through the parameter **instance** *instance-id*. The current device will be assigned as the root bridge or backup bridge of CIST if instance-id is 0 or parameter **instance** *instance-id* is omitted.
- The roots in device instances are independent mutually, that is to say, they cannot only be the root bridge or backup bridge of one instance, but also the root bridge or backup bridge of other spanning tree instances. However, in the same spanning tree instance, the same device cannot be used as the root bridge and backup bridge at the same time.
- You cannot assign two or more root bridges for one spanning tree instance, but can assign several backup bridges for one spanning tree. Generally speaking, you had better assign one root bridge and several backup bridges for a spanning tree.

2.7.7 Configuring device interface and system priority

Whether the interface is selected as the root interface depends on interface priority. Under the identical condition, the interface with smaller priority will be selected as the root interface. An interface may have different priorities and play different roles in different instances.

The Bridge ID decides whether the QSW-8200 series switch can be selected as the root of the spanning tree. Configuring smaller priority helps obtain smaller Bridge ID and designate the QSW-8200 series switch as the root. If priorities of two QSW-8200 series switch devices are identical, the QSW-8200 series switch with smaller MAC address will be selected as the root.

Similar to configuring root and backup root, priority is mutually independent in different instances. You can confirm priority instance through the **instance** *instance-id* parameter. Configure bridge priority for CIST if instance-id is 0 or the **instance** *instance-id* parameter is omitted.

Configure interface priority and system priority for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**spanning-tree** [**instance** *instance-id*] **priority** *priority-value* Qtech(config-port)#**exit**	Set interface priority for a STP instance.
4	Qtech(config)#**spanning-tree** [**instance** *instance-id*] **priority** *priority-value*	Set system priority for a STP instance.

Note

The value of priority must be multiples of 4096, like 0, 4096, 8192, etc. It is 32768 by default.

2.7.8 Configuring network diameter for switching network

The network diameter indicates the number of nodes on the path that has the most devices on a switching network. In MSTP, the network diameter is valid only to CIST, and invalid to MSTI instance. No matter how many nodes in a path in one domain, it is considered as just one node. Actually, network diameter should be defined as the domain number in the path crossing the most domains. The network diameter is 1 if there is only one domain in the whole network.

The maximum number of hops of MST domain is used to measure the domain scale, while network diameter is a parameter to measure the whole network scale. The bigger the network diameter is, the bigger the network scale is.

Similar to the maximum number of hops of MST domain, only when the QSW-8200 series switch is configured as the CIST root device can this configuration take effect. MSTP will automatically set the Hello Time, Forward Delay and Max Age parameters to a privileged value through calculation when configuring the network diameter.

Configure the network diameter for the switching network as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`spanning-tree bridge-diameter`** *`bridge-diameter-value`*	Configure the network diameter for the switching network.

2.7.9 Configuring inner path cost for interfaces

When selecting the root interface and designated interface, the smaller the interface path cost is, the easier it is to be selected as the root interface or designated interface. Inner path costs of interface are independently mutually in different instances. You can configure inner path cost for instance through the **instance** *instance-id* parameter. Configure inner path cost of interface for CIST if instance-id is 0 or the **instance** *instance-id* parameter is omitted.

By default, interface cost often depends on the physical features:

- 10 Mbit/s: 2000000
- 100 Mbit/s: 200000
- 1000 Mbit/s: 20000
- 10 Gbit/s: 2000

Configure the inner path cost for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Qtech(config-port)#`**`spanning-tree`** `[` **`instance`** *`instance-id`* `]` **`inter-path-cost`** *`cost-value`*	Configure the inner path cost on the interface.

2.7.10 Configuring external path cost on interface

The external path cost is the cost from the device to the CIST root, which is equal in the same domain.

Configure the external path cost for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Qtech(config-port)#`**`spanning-tree extern-path-cost`** *`cost-value`*	Configure the external path cost on interface.

2.7.11 Configuring maximum transmission rate on interface

The maximum transmission rate on an interface means the maximum number of transmitted BPDUs allowed by MSTP in each Hello Time. This parameter is a relative value and of no unit. The greater the parameter is configured, the more packets are allowed to be transmitted in a Hello Time, the more device resources it takes up. Similar with the time parameter, only the configurations on the root device can take effect.

Configure maximum transmission rate on the interface for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`spanning-tree transit-limit`** *`value`*	Configure interface maximum transmission rate.

2.7.12 Configuring MSTP timer

- Hello Time: the QSW-8200 series switch sends the interval of bridge configurations (BPDU) regularly to check whether there is failure in detection link of the QSW-8200 series switch. The QSW-8200 series switch sends hello packets to other devices around in Hello Time to check if there is fault in the link. The default value is 2s. You can adjust the interval value according to network condition. Reduce the interval when network link changes frequently to enhance the stability of STP. However, increasing the interval reduces CPU utilization rate for STP.
- Forward Delay: the time parameter to ensure the safe transit of device status. Link fault causes the network to recalculate spanning tree, but the new configuration message recalculated cannot be transmitted to the whole network immediately. There may be temporary loop if the new root interface and designated interface start transmitting data at once. This protocol adopts status remove system: before the root interface and designated interface starts forwarding data, it needs a medium status (learning status); after delay for the interval of Forward Delay, it enters forwarding status. The delay guarantees the new configuration message to be transmitted through whole network. You

can adjust the delay according to actual condition; namely, reduce it when network topology changes infrequently and increase it under opposite conditions.

- Max Age: the bridge configurations used by STP have a life time that is used to judge whether the configurations are outdated. The QSW-8200 series switch will discard outdated configurations and STP will recalculate spanning tree. The default value is 20s. Over short age may cause frequent recalculation of the spanning tree, while over greater age value will make STP not adapt to network topology change timely.

All devices in the whole switching network adopt the three time parameters on CIST root device, so only the root device configuration is valid.

Configure the MSTP timer for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`spanning-tree hello-time`** *`value`*	Set Hello Time.
3	`Qtech(config)#`**`spanning-tree forward-delay`** *`value`*	Set Forward Delay.
4	`Qtech(config)#`**`spanning-tree max-age`** *`value`*	Set Max Age.

2.7.13 Configuring edge interface

The edge interface indicates the interface neither directly connects to any devices nor indirectly connects to any device via network.

The edge interface can change the interface status to forward quickly without any waiting time. You had better set the Ethernet interface connected to user client as edge interface to make it quick to change to forward status.

The edge interface attribute depends on actual condition when it is in auto-detection mode; the real port will change to false edge interface after receiving BPDU when it is in force-true mode; when the interface is in force-false mode, whether it is true or false edge interface in real operation, it will maintain the force-false mode until the configuration is changed.

By default, all interfaces on the QSW-8200 series switch are set in auto-detection attribute.

Configure the edge interface for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Qtech(config-port)#`**`spanning-tree edged-port`** `{` **`auto`** `|` **`force-true`** `|` **`force-false`** `}`	Configure attributes of the RSTP edge interface.

2.7.14 Configuring link type

Two interfaces connected by a point-to-point link can quickly transit to forward status by transmitting synchronization packets. By default, MSTP configures the link type of interfaces according to duplex mode. The full duplex interface is considered as the point-to-point link, and the half duplex interface is considered as the shared link.

You can manually configure the current Ethernet interface to connect to a a point-to-point link, but the system will fail if the link is not point to point. Generally, we recommend configure this item in auto status and the system will automatically detect whether the interface is connected to a point-to-point link.

Configure link type for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Qtech(config-port)#`**`spanning-tree link-type`** `{` **`auto`** `|` **`point-to-point`** `|` **`shared`** `}`	Configure link type for interface.

2.7.15 Configuring root interface protection

The network will select a bridge again when it receives a packet with higher priority, which influents network connectivity and also consumes CPU resource. For the MSTP network, if someone sends BPDUs with higher priority, the network may become unstable for the continuous election.

Generally, priority of each bridge has already been configured in network planning phase. The nearer a bridge is to the edge, the lower the bridge priority is. So the downlink interface cannot receive the packets higher than bridge priority unless under someone attacks. For these interfaces, you can enable rootguard to refuse to process packets with priority higher than bridge priority and block the interface for a period to prevent other attacks from attacking sources and damaging the upper layer link.

Configure root interface protection for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Qtech(config-port)#`**`spanning-tree rootguard`** `{` **`enable`** `|` **`disable`** `}`	Configure root interface protection.

2.7.16 Configuring interface loopguard

The spanning tree has two functions: loopguard and link backup. Loopguard requires carving up the network topology into tree structure. There must be redundant link in the topology if link backup is required. Spanning tree can avoid loop by blocking the redundant link and enable link backup function by opening redundant link when the link breaks down.

The spanning tree module exchanges packets periodically, and the link has failed if it has not received packet in a period. Then select a new link and enable backup interface. In actual networking, the cause to failure in receiving packets may not link fault. In this case, enabling the backup interface may lead to loop.

Loopguard is used to keep the original interface status when it cannot receive packet in a period.

Note

Loopguard and link backup are mutually exclusive; namely, loopguard is implemented on the cost of disabling link backup.

Configure interface loop protection for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**spanning-tree loopguard { enable | disable }**	Configure interface loopguard attributes.

2.7.17 Executing mcheck operation

Interface on MSTP device has two working modes: STP compatible mode and MSTP mode. Suppose the interface of MSTP device in a switch network is connected to the QSW-8200 series switch running STP, the interface will change to work in STP compatible mode automatically. But the interface cannot change to work in MSTP mode if the QSW-8200 series switch running STP is removed, i.e. the interface still works in STP compatible mode. You can execute the **mcheck** command to force the interface working in MSTP mode. If the interface receives new STP packet again, it will return to STP compatible mode.

Execute mcheck operation for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**spanning-tree mcheck**	Execute mcheck operation, force to remove interface to MSTP mode.

2.7.18 Checking configurations

Use the following commands to check configuration results.

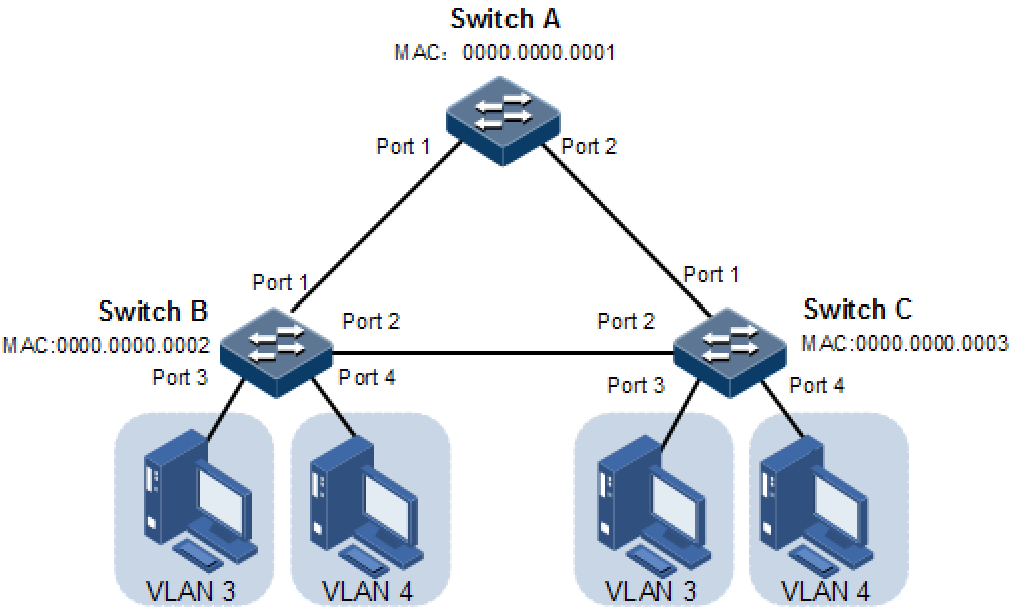
No.	Command	Description
1	`Qtech#show spanning-tree`	Show basic configurations of STP.
2	`Qtech#show spanning-tree [ instance instance-id ] port-list port-list [ detail ]`	Show configurations of spanning tree on the interface.
3	`Qtech#show spanning-tree region-operation`	Show configurations of the MST domain.

2.7.19 Example for configuring MSTP

Networking requirements

As shown in Figure 2-17, three QSW-8200 series switch devices are connected to form a ring network through MSTP, with the domain name aaa. Switch B, connected with a PC, belongs to VLAN 3. Switch C, connected with another PC, belongs to VLAN 4. Instant 3 is related to VLAN 3. Instant 4 is related to VLAN 4. Configure the path cost of instance 3 on Switch B so that packets of VLAN 3 and VLAN 4 are forwarded respectively in two paths, which eliminates loopback and implements load sharing.

Figure 2-17 MSTP networking



Configuration steps

Step 1 Create VLAN 3 and VLAN 4 on Switch A, Switch B, and switch C respectively, and activate them.

Configure Switch A.

```
Qtech#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 3-4 active
```

Configure Switch B.

```
Qtech#hostname SwitchB
SwitchB#config
SwitchB(config)#create vlan 3-4 active
```

Configure Switch C.

```
Qtech#hostname SwitchC
SwitchC#config
SwitchC(config)#create vlan 3-4 active
```

Step 2 Configure Port 1 and Port 2 on Switch A to allow all VLAN packets to pass in Trunk mode. Configure Port 1 and Port 2 on Switch B to allow all VLAN packets to pass in Trunk mode. Configure Port 1 and Port 2 on Switch C to allow all VLAN packets to pass in Trunk mode. Configure Port 3 and Port 4 on Switch B and Switch C to allow packets of VLAN 3 and VLAN 4 to pass in Access mode.

Configure Switch A.

```
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#exit
SwitchA(config)#interface port 2
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#exit
```

Configure Switch B.

```
SwitchB(config)#interface port 1
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#exit
SwitchB(config)#interface port 2
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#exit
SwitchB(config)#interface port 3
SwitchB(config-port)#switchport access vlan 3
SwitchB(config-port)#exit
SwitchB(config)#interface port 4
SwitchB(config-port)#switchport access vlan 4
SwitchB(config-port)#exit
```

Configure Switch C.

```
SwitchC(config)#interface port 1
SwitchC(config-port)#switchport mode trunk
SwitchC(config-port)#exit
SwitchC(config)#interface port 2
SwitchC(config-port)#switchport mode trunk
SwitchC(config-port)#exit
SwitchC(config)#interface port 3
SwitchC(config-port)#switchport access vlan 3
SwitchC(config-port)#exit
SwitchC(config)#interface port 4
SwitchC(config-port)#switchport access vlan 4
SwitchC(config-port)#exit
```

Step 3 Set spanning tree mode of Switch A, Switch B, and Switch C to MSTP, and enable STP. Enter MSTP configuration mode, and set the domain name to aaa, revised version to 0. Map instance 3 to VLAN 3, and instance 4 to VLAN 4. Exist from MST configuration mode.

Configure Switch A.

```
SwitchA(config)#spanning-tree mode mstp
SwitchA(config)#spanning-tree enable
SwitchA(config)#spanning-tree region-configuration
SwitchA(config-region)#name aaa
SwitchA(config-region)#revision-level 0
SwitchA(config-region)#instance 3 vlan 3
SwitchA(config-region)#instance 4 vlan 4
```

Configure Switch B.

```
SwitchB(config)#spanning-tree mode mstp
SwitchB(config)#spanning-tree enable
SwitchB(config)#spanning-tree region-configuration
SwitchB(config-region)#name aaa
SwitchB(config-region)#revision-level 0
SwitchB(config-region)#instance 3 vlan 3
SwitchB(config-region)#instance 4 vlan 4
SwitchB(config-region)#exit
```

Configure Switch C.

```
SwitchC(config)#spanning-tree mode mstp
SwitchC(config)#spanning-tree enable
SwitchC(config)#spanning-tree region-configuration
SwitchC(config-region)#name aaa
SwitchC(config-region)#revision-level 0
SwitchC(config-region)#instance 3 vlan 3
SwitchC(config-region)#instance 4 vlan 4
```

Step 4 Set the inner path coast of Port 1 of spanning tree instance 3 to 500000 on Switch B.

```
SwitchB(config)#interface port 1
SwitchB(config-port)#spanning-tree instance 3 inter-path-cost 500000
```

Checking results

Use the **show spanning-tree region-operation** command to show configurations of the MST domain.

```
Qtech#show spanning-tree region-operation
Operational Information:
-----------------------------------------------
Name: aaa
Revision level: 0
Instances running: 3
Digest: 0X7D28E66FDC1C693C1CC1F6B61C1431C4
Instance     Vlans Mapped
--------     ----------------------
0          1,2,5-4094
3          3
4          4
```

Use the **show spanning-tree instance 3** command to check whether basic information about spanning tree instance 3 is correct.

- Switch A

```
SwitchA#show spanning-tree instance 3
Spanning-tree admin state: enable
Spanning-tree protocol mode: MSTP
MST ID: 3
-----------------------------------------------------------
BridgeId:    Mac 0000.0000.0001  Priority 32768
RegionalRoot: Mac 0000.0000.0001  Priority 32768   InternalRootCost 0
PortId  PortState   PortRole   PathCost  PortPriority  LinkType   TrunkPort
------------------------------------------------------------------------
P1      forwarding  designated 200000    128         point-to-point  no
P2      forwarding  designated 200000    128         point-to-point  no
```

- Switch B

```
SwitchB#show spanning-tree instance 3
Spanning-tree admin state: enable
Spanning-tree protocol mode: MSTP
MST ID: 3
```

```
-----------------------------------------------------------
BridgeId:    Mac 0000.0000.0002  Priority 32768
RegionalRoot: Mac 0000.0000.0001  Priority 32768   InternalRootCost
500000
PortId  PortState   PortRole   PathCost  PortPriority  LinkType   TrunkPort
-------------------------------------------------------------------------
1      discarding  alternate  500000    128         point-to-point  no
3      forwarding  root      200000    128         point-to-point  no
…
```

- Switch C

```
SwitchC#show spanning-tree instance 3
Spanning-tree admin state: enable
Spanning-tree protocol mode: MSTP
MST ID: 3
-----------------------------------------------------------
BridgeId:    Mac 0000.0000.0003  Priority 32768
RegionalRoot: Mac 0000.0000.0001  Priority 32768   InternalRootCost
200000
PortId  PortState   PortRole   PathCost  PortPriority  LinkType   TrunkPort
-------------------------------------------------------------------------
2      forwarding  root       200000    128        point-to-point  no
3      forwarding  designated 200000    128         point-to-point  no
…
```

Use the **show spanning-tree instance 4** command to check whether basic information about spanning tree instance 4 is correct.

- Switch A

```
SwitchA#show spanning-tree instance 4
Spanning-tree admin state: enable
Spanning-tree protocol mode: MSTP
MST ID: 4
-----------------------------------------------------------
BridgeId:    Mac 001F.CE00.0000  Priority 32768
RegionalRoot: Mac 001F.CE00.0000  Priority 32768  InternalRootCost 0
Port    PortState  PortRole   PathCost  PortPriority  LinkType    TrunkPort
-------------------------------------------------------------------------
1     discarding  disabled   200000    128         point-to-point  yes
2     disabled   disabled   200000    128        point-to-point  yes
…
```

- Switch B

```
SwitchB#show spanning-tree instance 4
Spanning-tree admin state: enable
Spanning-tree protocol mode: MSTP
MST ID: 4
```

```
-------------------------------------------------------------
BridgeId:    Mac 0000.0000.0002  Priority 32768
RegionalRoot: Mac 0000.0000.0001  Priority 32768   InternalRootCost
200000
PortId  PortState   PortRole   PathCost  PortPriority  LinkType   TrunkPort
----------------------------------------------------------------------------
1      forwarding  root      200000   128        point-to-point  no
3      forwarding  designated 200000   128        point-to-point  no
…
```

- Switch C

```
SwitchC#show spanning-tree instance 4
Spanning-tree admin state: enable
Spanning-tree protocol mode: MSTP
MST ID: 4
-------------------------------------------------------------
BridgeId:    Mac 0000.0000.0003  Priority 32768
RegionalRoot: Mac 0000.0000.0001  Priority 32768   InternalRootCost
200000
PortId  PortState   PortRole   PathCost  PortPriority  LinkType  TrunkPort
----------------------------------------------------------------------------
2      forwarding  root      200000   128        point-to-point  no
3      discarding  alternate  200000   128        point-to-point  no
…
```

2.8 Loopback detection

2.8.1 Introduction

Loopback detection is used to eliminate impact on the network and improve network error-detection, error tolerance, and stability.

The procedure of loopback detection is as below:

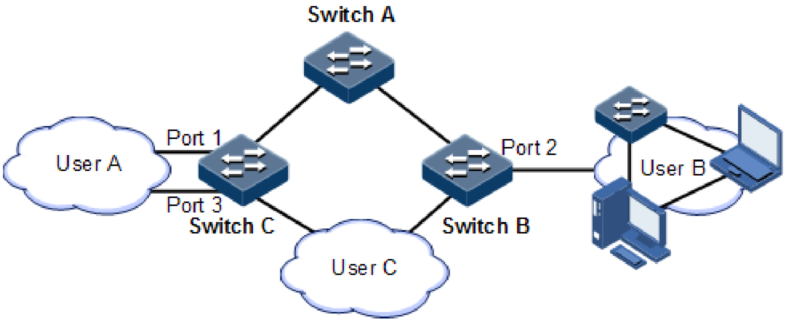
- Each interface of the device sends loopback detection packet at a certain interval (configurable, being 4s by default).
- The device checks source MAC field for a loopback detection packet received on the interface. If the source MAC is identical to the device MAC, it is supposed that a loop has formed on an interface; otherwise, discard the packet.
- If the packets Tx interface number is identical to Rx interface number, shut down the interface;
- If the packets Tx interface number is not identical to Rx interface number, shut down the interface with the bigger ID, and leave the interface with smaller ID in Up status.

Common loop types are self-loop, internal loop and external loop.

As shown in Figure 2-18, Switch B and Switch C, as edge switches, connect to the user network.

- Self-loop: user loop on the same Ethernet interface on the same device. User network B has a loop, which is self-loop, as shown in Figure 2-18.
- Internal loop: the loop forming on different Ethernet interfaces on the same device. Interface 1 and interface 3 of Switch C form internal loop with the user network A, as shown in Figure 2-18.
- External loop: the loop forming in the Ethernet interfaces on different devices, Switch A, Switch B and Switch C form external loop with user network C, as shown in Figure 2-18.

Figure 2-18 Principle of loopback detection



In Figure 2-18, assume that Switch B and Switch C interfaces connected to user network are enabled with loopback detection. The loop detection processing mechanism for the three loop types are as follows:

- Self-loop: the port IDs for receiving and sending packets on Switch B are the same, so shut down Port 2 to remove self-loop.
- Internal loop: Switch C receives loop detection packets sent by it and the port IDs for receiving and sending packets are different, so shut down Port 3 which has the bigger port ID to remove the internal loop.
- External loop: Switch B and Switch C receive the loop detection packets from each other; generally, loop detection does not process external loop, Switch B and Switch C only send Trap without blocking. But you can configure to block one of the ports manually, such as blocking the port with the bigger MAC address to remove external loop.

2.8.2 Preparing for configurations

Scenario

On the network, the hosts or Layer 2 devices connected under access devices may form loop through network cable intentionally or involuntary. Enable loopback detection on the downlink interface of the access device to avoid network jam forming by unlimited copies of data flow caused by downlink interface loop. Block the loop interface once there is a loop.

Prerequisite

- Connect interfaces.
- Configure physical parameters to make interfaces Up at the physical layer.

2.8.3 Default configurations of loopback detection

Default configurations of loopback detection are as below.

Function	Default value
Interface loopback detection status	Disable
Automatic recovery time for the blocked interface	No automatic recovery
Loop processing mode for loopback detection	trap-only
Loopback detection period	4s
Loopback detection mode	VLAN
Time for recovering the block interface due to loopback detection	Infinite

2.8.4 Configuring loopback detection

Note

- Loopback detection and STP are exclusive, only one can be enabled at a time.
- The straightly connected device cannot be enabled with loopback detection at both ends simultaneously; otherwise the interfaces at both ends will be blocked.

Configure loopback detection for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**loopback-detection** { **enable** | **disable** }*interface-type interface-number*	Configure loopback detection on the interface.
3	Qtech(config)#**loopback-detection hello-time** *period*	Configure the period for sending loopback detection packets.
4	Qtech(config)#**loopback-detection mode** { **port-based** | **vlan-based** }	(Optional) configure loopback detection mode.
5	Qtech(config)#**loopback-detection loop** { **discarding** | **trap-only** }*interface-type interface-number*	(Optional) configure processing mode when the interface receives loopback detection packets from other devices.
6	Qtech(config)#**loopback-detection down-time** { *time-value* | **infinite** }	(Optional) configure the automatic open blocked interface time for loopback detection.
7	Qtech(config)#**no loopback-detection discarding** *interface-type interface-number*	Enable the interface blocked by loopback detection.

2.8.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show loopback-detection** [*interface-type interface-number*]	Show configurations of loopback on the interface.
2	Qtech#**show loopback-detection block-vlan** [*interface-type interface-number*]	Show information about the VLAN blocked by loopback detection.

2.8.6 Maintenance

Maintain the QSW-8200 series switch as below.

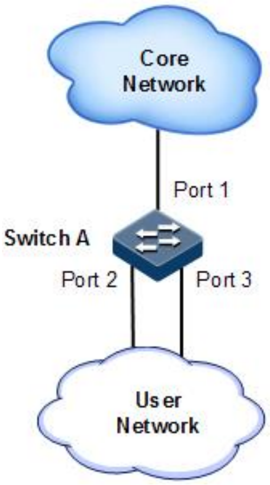
Command	Description
Qtech(config-port)#**clear loopback-detection statistic**	Clear loopback detection statistics.
Qtech(config-aggregator)#**clear loopback-detection statistic**	

2.8.7 Example for configuring loopback detection

Networking requirements

As shown in Figure 2-19, port 1 on Switch A is connected to the core network; port 2 and port 3 on Switch A are connected to the user network. There is loop on the user network. Enable loopback detection on Switch A to detect loop on the user network and then can block the related interface.

Figure 2-19 Loopback detection networking



Configuration steps

Step 1 Create VLAN 3, and add port 2 and port 3 into VLAN 3.

```
Qtech#config
Qtech(config)#create vlan 3 active
Qtech(config)#interface port 2
Qtech(config-port)#switchport access vlan 3
Qtech(config-port)#exit
Qtech(config)#interface port 3
Qtech(config-port)#switchport access vlan 3
Qtech(config-port)#exit
```

Step 2 Enable loopback detection for the specified interface.

```
Qtech(config)#loopback-detection enable port-list 2-3
Qtech(config)#loopback-detection hello-time 3
```

Checking results

Use the **show loopback-detection** command to show configurations of loopback detection.

```
Qtech#show loopback-detection port-list 2-3
Destination address: ffff.ffff.ffff
Mode:Vlan-based
Period of loopback-detection:3s
Restore time:infinite
Port              State    Status     loop      vlanlist
--------------------------------------------------------------
P2             Ena      no        trap-only  --
```

2.9 Interface protection

2.9.1 Introduction

Layer 2 data isolation is needed among different interfaces and interfaces are added to different VLANs. Sometimes interfaces in the same VLAN also need to be isolated by interface protection, which can isolate interfaces in a VLAN.

Through interface protection, you can enable interface protection on the interfaces that need to be controlled to achieve Layer 2 data isolation and implement equal physical isolation effect among interfaces, which improves network security and provides flexible networking solution to you.

Interfaces enabled with interface protection cannot communicate with each other, but An interface enabled with interface protection and an interface disabled with interface protection can still communicate with each other.

2.9.2 Preparing for configurations

Scenario

You need to configure interface protection to implement Layer 2 data isolation in the same VLAN and get the physical isolation effect among interfaces.

The interface protection function can realize mutual isolation of interfaces in the same VLAN, enhance network security, and provide flexible networking solutions for you.

Prerequisite

N/A

2.9.3 Default configurations of interface protection

Default configurations for interface protection are as below.

Function	Default value
Interface protection status of each interface	Disable

2.9.4 Configuring interface protection

Configure interface protection for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Qtech(config-port)#`**`switchport protect`**	Enable interface protection.

2.9.5 Checking configurations

Use the following commands to check configuration results.

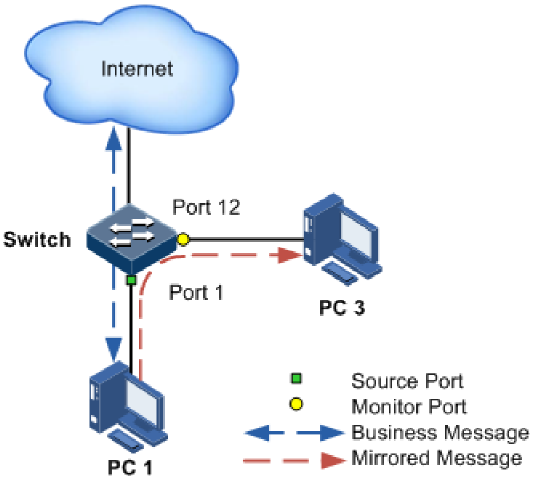
No.	Command	Description
1	`Qtech#`**`show switchport protect`**	Show configurations of interface protection.

2.10 Port mirroring

2.10.1 Introduction

Port mirroring refers to assigning some packets mirrored from the source interface to the destination interface, such as from the monitor port without affecting the normal packet forwarding. You can monitor sending and receiving status for packets on an interface through this function and analyze the relevant network conditions.

Figure 2-20 Principle of port mirroring



The basic principle of port mirroring is shown in Figure 2-20. PC 1 connects to the external network through port 1; PC 3 is the monitor PC, connecting to the external network through port 2.

When monitoring packets from the PC 1, you need to assign port 1 to be connected to PC 1 as the mirroring source port, enable port mirroring on the ingress port 1 and assign port 2 as the monitor port, namely, mirroring destination port.

When the service packets from PC 1 enter the device, the device forwards and copies them to the monitor port (port 2). The monitor device connected to the monitor port can receive and analyze these mirrored packets.

The QSW-8200 series switch supports data stream mirroring on the ingress port and the egress port. The packets on the ingress/egress mirroring port will be copied to the monitor port after port mirroring is enabled. The monitor port and mirroring port cannot be the same one.

2.10.2 Preparing for configurations

Scenario

Port mirroring is used to monitor network data type and flow regularly by the network administrator.

Port mirroring is to copy the interface flow monitored to a monitor port or CPU to obtain the ingress/the egress port failure or abnormal flow of data to analyze, discover the root cause and solve them timely.

Prerequisite

N/A

2.10.3 Default configurations of port mirroring

Default configurations of port mirroring are as below.

Function	Default value
Port mirroring status	Disable
Mirroring source port	N/A
Monitor port	port 1

Note

The output of the monitor port is null when packets are mirrored to the CPU.

2.10.4 Configuring port mirroring on local port

Caution

- There can be multiple source mirroring ports but only one monitor port.
- Packets of the ingress/egress mirroring port are copied to the monitor port after port mirroring takes effect. The monitor port cannot be set to the mirroring port again.

Configure local port mirroring for the QSW-8200 series switch as below.

Step	Configure	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**mirror** { **monitor-cpu** | **monitor-port** *port-id* }	Configure the mirroring port to mirror packets to the CPU or specified monitor port.
3	Qtech(config)#**mirror source-port-list** { **both port-list** *port-list* | **egress port-list** *port-list* | **ingress port-list** *port-list* }	Configure the mirror source port for port mirroring, and specify the mirror rule for port mirroring.
4	Qtech(config)#**mirror enable**	Enable port mirroring.

2.10.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Qtech#show mirror`	Show configurations of port mirroring.

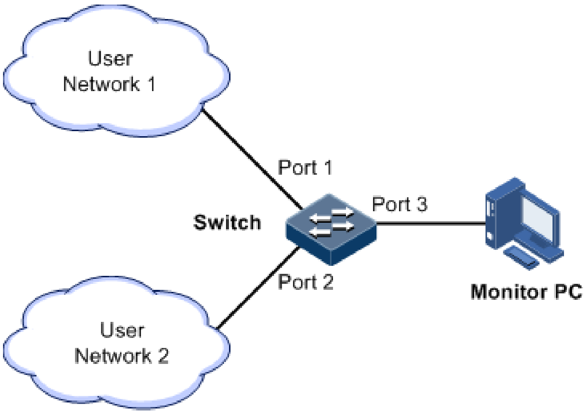
2.10.6 Example for configuring port mirroring

Networking requirements

As shown in Figure 2-21, the network administrator wishes to monitor user network 1 through a data monitor device, then catches the fault or abnormal data flow for analyzing and discovering problem and then solves it.

The QSW-8200 series switch is disabled with storm control and automatic packets sending. User network 1 accesses the QSW-8200 series switch through port 1, user network 2 accesses the QSW-8200 series switch through port 2, and the data monitor device is connected to port 3.

Figure 2-21 Port mirroring networking



Configuration steps

Enable port mirroring on the Switch.

```
Qtech#config
Qtech(config)#mirror monitor-port port 3
Qtech(config)#mirror source-port-list both port-list 1
Qtech(config)#mirror enable
```

Checking results

Use the **show mirror** command to show configurations of port mirroring.

```
Qtech#show mirror
Mirror: Enable
Monitor port: port3
```

```
Remote Vlan: --
-----------the ingress mirror rule-----------
Mirrored ports: port-list 1
-----------the egress mirror rule-----------
Mirrored ports: port-list 1
```

2.11 L2CP

2.11.1 Introduction

Metro Ethernet Forum (MEF) introduces service concepts, such as EPL, EVPL, EP-LAN, and EVP-LAN. Different service types have different processing modes for Layer 2 Control Protocol (L2CP) packets.

MEF6.1 defines processing modes for L2CP as below.

- Discard: discard the packet, by applying the configured L2CP profile on the ingress interface of the QSW-8200 series switch, to complete configuring processing mode.
- Peer: send packets to the CPU in the same way as the discard action.
- Tunnel: send packets to the MAN. It is more complex than discard and peer mode, requiring cooperating profile at network side interface and carrier side interface tunnel terminal to allow packets to pass through the carrier network.

2.11.2 Preparing for configurations

Preparing for configurations

On the access device of MAN, you can configure profile on user network interface according to services from the carrier to configure L2CP of the user network.

Preparation

N/A

2.11.3 Defaul configurations of L2CP

Default configurations of L2CP are as below.

Function	Default value
Global L2CP status	Disable
Applying the profile on the interface	Disable
Port tunnel terminal status	Disable
Specify multicast destination MAC address	0x0100.0ccd.cdd0
Description of L2CP profile	N/A

2.11.4 Configuring global L2CP

Configure global L2CP for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**l2cp enable**	Enable global L2CP.
3	Qtech(config)#**l2cp dest-mac** *mac-address*	Configure the specified multicast destination MAC address.

2.11.5 Configuring L2CP profile

Configure the L2CP profile for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**l2cp-profile** *profile-number*	Create and enter the L2CP profile.
3	Qtech(config-l2cpprofile)#**description** *string*	(Optional) add profile description.
4	Qtech(config-l2cpprofile)#**l2cp** { *mac-address* | **all** } { **cos** *cos* | **peer** | **discard** | **forward-statistics** }	(Optional) configure the process action for L2CP packets.
	Qtech(config-l2cpprofile)#**l2cp** { **cisco** | **dot1x** | **elmi** | **lldp** | **slow-protocol** | **stp** } { **cos** *cos* | **peer** | **discard** | **tunnel** | **forward-statistics** }	
	Qtech(config-l2cpprofile)#**l2cp** { **esmc** | **lacp** | **lamp** | **link-oam** } { **peer** | **discard** | **tunnel** | **forward-statistics** }	

2.11.6 Configuring interface L2CP

Configure interface L2CP for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical interface configuration mode.

Step	Command	Description
3	Qtech(config-port)#**l2cp profile** *profile-number*	Apply the L2CP profile on the interface.
	Qtech(config-port)#**l2cp tunnel-terminal**	(Optional) configure the interface as the Tunnel terminal. To enable L2CP to process packets in Tunnel transparent transmission, configure the interface as the Tunnel terminal.
4	Qtech(config-port)#**l2cp peer vlan** *vlan-id*	(Optional) configure the interface to send packets of the specified VLAN to the CPU.

Note

Applying a profile to an interface takes effect unless global L2CP is enabled. You can configure it but it will not take effect if global L2CP is disabled. The configuration takes effect once global L2CP is enabled.

2.11.7 Checking configurations

Use the following commands check configuration results.

No.	Command	Description
1	Qtech#**show l2cp-profile** [*profile-number*]	Show information about the created L2CP profile.
2	Qtech#**show l2cp** [**port-list** *port-list*]	Show configurations of L2CP on the interface.
3	Qtech#**show l2cp statistic** [**port-list** *port-list*]	Show statistics of L2CP packets on the interface.

2.11.8 Maintenance

Maintain the QSW-8200 series switch as below.

Command	Description
Qtech(config)#**clear l2cp statistic** [**port-list** *port-list*]	Clear statistics of L2CP packets on the interface.

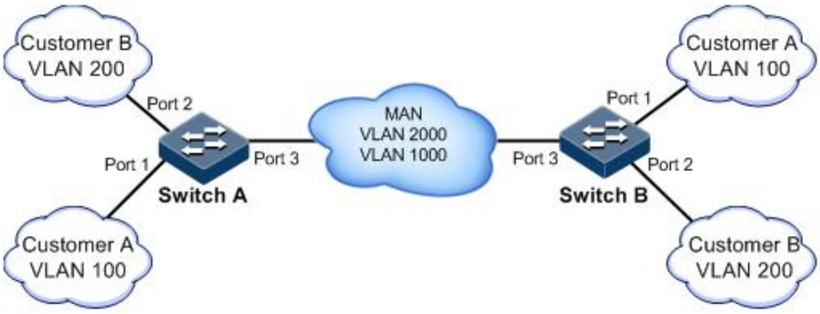
2.11.9 Example for configuring L2CP

Networking requirements

As shown in Figure 2-22, configure L2CP on Switch A and Switch B as below.

- Specify the multicast destination MAC address of them to 0100.1234.1234.
- Configure the STP packets of Customer A to pass through the MAN, and discard other packets.
- Configure the STP and VTP packets of Customer B to pass through the MAN, send elmi packets to the CPU, and discard other packets.

Figure 2-22 L2CP networking



Configuration steps

Configure Switch A and Switch B.

Configurations of Switch A and Switch B are identical. Take Switch A for example.

Step 1 Enable global L2CP.

```
Qtech#hostname SwitchA
Qtech#config
Qtech(config)#l2cp enable
```

Step 2 Configure the specified multicast destination MAC address.

```
Qtech(config)#l2cp dest-mac 0100.1234.1234
```

Step 3 Configure L2CP profile 1, and apply the profile to port 1 for Customer A.

```
Qtech(config)#l2cp-profile 1
Qtech(config-l2cpproflie)#description CustomerA
Qtech(config-l2cpproflie)#l2cp all discard
Qtech(config-l2cpproflie)#l2cp stp tunnel
Qtech(config-l2cpproflie)#exit
Qtech(config)#interface port 1
Qtech(config-port)#l2cp profile 1
Qtech(config-port)#exit
```

Step 4 Configure L2CP profile 2, and apply the profile to port 2 for Customer B.

```
Qtech(config)#l2cp-profile 2
Qtech(config-l2cpproflie)#description CustomerB
Qtech(config-l2cpproflie)#l2cp all discard
Qtech(config-l2cpproflie)#l2cp stp tunnel
Qtech(config-l2cpproflie)#l2cp cisco tunnel
Qtech(config-l2cpproflie)#l2cp elmi peer
Qtech(config-l2cpproflie)#exit
Qtech(config)#interface port 2
Qtech(config-port)#l2cp profile 2
Qtech(config-port)#exit
```

Step 5 Configure port 3 to the tunnel terminal.

```
Qtech(config)#interface port 3
Qtech(config-port)#l2cp tunnel-terminal
```

Checking results

Use the **show l2cp-profile** command to show L2CP configurations.

```
Qtech#show l2cp-profile
Profile     Description              Reference   Protocol       Action
-------------------------------------------------------------------------
Profile1    customerA                 1         stp           tunnel
                                                slow-protocol   discard
                                                dot1x          discard
                                                elmi           discard
                                                lldp           discard
                                                cisco          discard
                                                0180.c200.0004   discard
                                                0180.c200.0005   discard
                                                0180.c200.0006   discard
                                                0180.c200.0008   discard
                                                0180.c200.0009   discard
                                                0180.c200.000a   discard
                                                0180.c200.000b   discard
                                                0180.c200.000c   discard
                                                0180.c200.000d   discard
                                                0180.c200.000f   discard
                                                0180.c200.0020   discard
Profile2    customerB                 1         stp           tunnel
                                                slow-protocol   discard
                                                dot1x          discard
                                                elmi           peer
                                                lldp           discard
                                                cisco          tunnel
                                                0180.c200.0004  discard
                                                0180.c200.0005  discard
                                                0180.c200.0006  discard
                                                0180.c200.0008  discard
                                                0180.c200.0009  discard
                                                0180.c200.000a  discard
                                                0180.c200.000b  discard
                                                0180.c200.000c  discard
                                                0180.c200.000d  discard
                                                0180.c200.000f  discard
                                                0180.c200.0020  discard

Default1    EPL_Option1& EP-LAN&EP-TREE     0         stp           --
…
```

Use the **show l2cp** command to show interface configurations.

```
Qtech#show l2cp
L2CP Status: Enable
Specified Destination MAC Address: 0100.1234.1234
Port     ProfileID   Tunnel-terminal  Peer-vlanlist
------------------------------------------------------
P1      Profile1    Disable        --
P2      Profile2    Disable        --
P3      --         Enable        --
…
```

2.12 Layer 2 protocol transparent transmission

2.12.1 Introduction

Transparent transmission is one of the main Ethernet device functions, and usually the edge network devices of carrier conduct Layer 2 protocol packet transparent transmission. Transparent transmission is enabled on the interface that connects edge network devices of carrier and user network. The interface is in Access mode, connecting to Trunk interface on user device. The layer 2 protocol packet of the user network is send from transparent transmission interface, encapsulated by the edge network device (ingress end of packets), and then send to the carrier network. The packet is transmitted through the carrier network to reach the edge device (egress end of packet) at the other end or carrier network. The edged device decapsulates outer layer 2 protocol packet and transparent transmits it to the user network.

The transparent transmission function includes packet encapsulation and decapsulation function, the basic implementing principle as below.

- Packet encapsulation: at the packet ingress end, the QSW-8200 series switch modifies the destination MAC address from user network layer 2 protocol packets to special multicast MAC address (it is 010E.5E00.0003 by default). On the carrier network, the modified packet is forwarded as data in customer VLAN.
- Packet decapsulation: at the packet egress end, the QSW-8200 series switch senses packet with special multicast MAC address (it is 010E.5E00.0003 by default), reverts the destination MAC address to DMAC of Layer 2 protocol packets, then sends the packet to assigned user network.

Layer 2 protocol transparent transmission can be enabled at the same time with QinQ or enabled independently. In actual networking, after modifying the MAC address of protocol packets, you need to add outer Tag for packets to send them through the carrier network.

The QSW-8200 series switch supports transparent transmission of BPDUs, DOT1X packet, LACP packet, CDP packet, PVST packet, PAGP packet, STP packet, UDLD packet, and VTP packet.

2.12.2 Preparing for configurations

Scenario

This function enables layer 2 protocol packets of one user network traverse the carrier network to make one user network in different regions uniformly running the same Layer 2 protocol. You can configure rate limiting on transparent transmission packets to prevent packet loss.

Prerequisite

Configure physical parameters for the interface to set it in Up status.

2.12.3 Default configurations of Layer 2 protocol transparent transmission

Default configurations of Layer 2 protocol transparent transmission are as below.

Function	Default value
Layer 2 protocol transparent transmission status	Disable
Egress interface and belonged VLAN of Layer 2 protocol packet	N/A
Tag CoS value of transparent transmission packet	5
Destination MAC address of transparent transmission packet	010E.5E00.0003
Discarding threshold and disabling threshold of transparent transmission packet	N/A

2.12.4 Configuring transparent transmission parameters

Configure transparent transmission parameter for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**relay destination-address** *mac-address*	(Optional) configure destination MAC for transparent transmission packets. By default, it is 010E.5E00.0003.
3	Qtech(config)#**relay cos** *cos-value*	(Optional) configure CoS value for transparent transmission packets.
4	Qtech(config)#**interface** *interface-type port-id*	Enter physical layer interface configuration mode or LAG configuration mode.
5	Qtech(config-port)#**relay** *interface-type interface-number* Qtech(config-aggregator)#**relay** *interface-type interface-number*	Configure specified egress interface for transparent transmission packets.
6	Qtech(config-port)#**relay vlan** *vlan-id* Qtech(config-aggregator)#**relay vlan** *vlan-id*	Configure specified VLAN for transparent transmission packets. This configuration enables packets to be forwarded according to the specified VLAN instead of the ingress interface.

7	Qtech(config-port)#**relay** { **all** | **cdp** | **dot1x** | **lacp** | **pagp** | **pvst** | **stp** | **udld** | **vtp** }
	Qtech(config-aggregator)#**relay** { **all** | **cdp** | **dot1x** | **lacp** | **pagp** | **pvst** | **stp** | **udld** | **vtp** }
		Configure the type of transparent transmission packets on the interface, and disable the corresponding protocol.

2.12.5 (Optional) configuring rate limiting for transparent transmission parameters

Configure rate limit for transparent transmission parameters for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**relay destination-address** *mac-address*	Enter physical layer interface configuration mode or LAG configuration mode.
3	Qtech(config-port)#**relay vlan** *vlan-id* Qtech(config-aggregator)#**relay vlan** *vlan-id*	Configure the threshold for discarding transparent transmission packets.
4	Qtech(config-port)#**relay** { **all** | **cdp** | **dot1x** | **lacp** | **pagp** | **pvst** | **stp** | **udld** | **vtp** }	Configure the threshold for shutting down the interface for transparent

Step	Command	Description
	Qtech(config-aggregator)#**relay { all | cdp | dot1x | lacp | pagp | pvst | stp | udld | vtp }**	transmission packets.

Note

The range of both the threshold for discarding transparent transmission packets and the threshold for shutting down the interface for transparent transmission packets is 1 to 4096. Usually, the former is smaller than the later.

2.12.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show relay** [*interface-type interface-number*]	Show configurations and status of transparent transmission.
2	Qtech#**show relay statistics** [*interface-type interface-number*]	Show statistics of transparent transmission packets.

2.12.7 Maintenance

Maintain the QSW-8200 series switch as below.

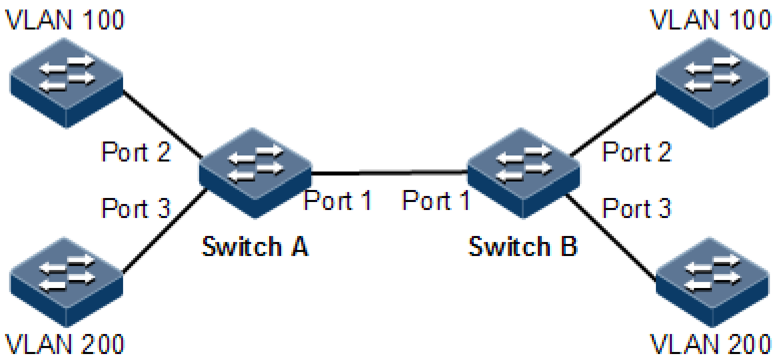
Commands	Description
Qtech(config)#**clear relay statistics** [*interface-type interface-number*]	Clear statistics of transparent transmission packets.

2.12.8 Example for configuring Layer 2 protocol transparent transmission

Networking requirements

As shown in Figure 2-23, Switch A and Switch B connect to two user networks VLAN 100 and VLAN 200 respectively. You need to configure Layer 2 protocol transparent transmission on Switch A and Switch B to make the same user network in different regions run STP entirely.

Figure 2-23 Layer 2 protocol transparent transmission networking



Configuration steps

Step 1 Create VLANs 100 and 200, and activate them.

Configure Switch A.

```
Qtech#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 100,200 active
```

Configure Switch B.

```
Qtech#hostname SwitchB
SwitchA#config
SwitchA(config)#create vlan 100,200 active
```

Step 2 Set the switching mode of Port 2 to Access mode, set the Access VLAN to 100, enable STP transparent transmission, and set the threshold for transparently transmitting STP packets to 1500.

Configure Switch A.

```
SwitchA(config)#interface port 2
SwitchA(config-port)#switchport mode access
SwitchA(config-port)#switchport access vlan 100
SwitchA(config-port)#relay stp
SwitchA(config-port)#relay port 1
SwitchA(config-port)#relay drop-threshold stp 1500
SwitchA(config-port)#exit
```

Configure Switch B.

```
SwitchB(config)#interface port 2
SwitchB(config-port)#switchport mode access
SwitchB(config-port)#switchport access vlan 100
SwitchB(config-port)#relay stp
SwitchB(config-port)#relay port 1
SwitchB(config-port)#relay drop-threshold stp 1500
SwitchB(config-port)#exit
```

Step 3 Set the switching mode of Port 3 to Access mode, set the Access VLAN to 200, and enable STP transparent transmission, and set the threshold for transparently transmitting STP packets to 1000.

Configure Switch A.

```
SwitchA(config)#interface port 3
SwitchA(config-port)#switchport mode access
SwitchA(config-port)#switchport access vlan 200
SwitchA(config-port)#relay stp
SwitchA(config-port)#relay port 1
SwitchA(config-port)#relay drop-threshold stp 1000
SwitchA(config-port)#exit
```

Configure Switch B.

```
SwitchB(config)#interface port 3
SwitchB(config-port)#switchport mode access
SwitchB(config-port)#switchport access vlan 200
SwitchB(config-port)#relay stp
SwitchB(config-port)#relay port 1
SwitchB(config-port)#relay drop-threshold stp 1000
SwitchB(config-port)#exit
```

Step 4 Set the switching mode of Port 1 to Trunk mode.

Configure Switch A.

```
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport mode trunk
```

Configure Switch B.

```
SwitchB(config)#interface port 1
SwitchB(config-port)#switchport mode trunk
```

Checking results

Use the **show relay** command to show configurations of Layer 2 protocol transparent transmission.

Take Switch A for example.

```
SwitchA#show relay port-list 1-3
COS for Encapsulated Packets: 5
Destination MAC Address for Encapsulated Packets: 010E.5E00.0003
Port    vlan  Egress-Port   Protocol     Drop-Threshold  Shutdown-Threshold
--------------------------------------------------------------------------
P1(up)    --    --          stp            --               --
                               dot1x          --               --
                                lacp           --               --
                                gvrp           --               --
                                cdp            --               --
                                vtp            --               --
                                pvst           --               --

P2(up)   --    P1       stp(enable)     1500            --
                              dot1x          --               --
                               lacp           --               --
                                gvrp           --               --
                                cdp            --               --
                                vtp            --               --
                                pvst           --               --

P3(up)   --    P1        stp(enable)    1000            --
                               dot1x          --               --
                               lacp           --               --
                               gvrp            --               --
                                cdp            --                --
                                vtp            --                --
                                pvst           --                --
```

2.13 GARP

2.13.1 Introduction

Generic Attribute Registration Protocol (GARP) provides a mechanism to help GARP members in the same switching network to distribute, broadcast, and register information (such as VLAN and multicast information).

Through GARP, configurations of a GARP member spread to the entire switching network. The GARP member can be a work station or bridge. It notifies other GARP member to register or deregister its attributes through declaration or withdrawal of declaration, and register or deregister attributes of the peer GARP member through declaration or withdrawal of declaration by the peer GARP.

GARP members exchange information by transmitting messages, including the following three types of messages:

- Join message: a GARP application entity sends out a Join message when it needs another device to register its attributes (such as VLAN information).
- Leave message: a GARP application entity sends out a Leave message when it needs another device to register its attributes.
- LeaveAll message: when the GARP application entity is started, the LeaveAll timer starts. It sends a LeaveAll message when this timer expires.

The Join message cooperates with the Leave message to guarantee deregistration and re-registration of messages. By exchanging messages, the QSW-8200 series switch can transmit attributes of messages to be registered to all switches in the same switching network.

The destination MAC address of packets of a GARP application entity is a specific multicast MAC address. After receiving packets of the GARP application entity, a GARP-supportive switch distinguishes them by their destination MAC addresses and thus transmits them to different GARP applications (GVRP or GMRP) for processing.

GVRP

GARP VLAN Registration Protocol (GVRP) is a GARP application. Based on GARP working mechanism, it maintains VLAN dynamic registration information about the switch, and sends the information to other switches.

All GVRP-supportive switches can receive VLAN registration information from other switches, and dynamically update local VLAN registration information, including current VLAN members and the port through which the VLAN member is reachable. In addition, all GVRP-supportive switches can send local VLAN registration information to other switches so that they have consistent VLAN registration information in the same VLAN.

2.13.2 Preparing for configurations

Scenario

Through GVRP, the QSW-8200 series switch can exchange VLAN configurations with other GVRP-enabled devices, discard unnecessary broadcast and unknown unicast traffic in the IEEE 802.1Q Trunk link, and dynamically create and manage VLANs.

Prerequisite

Configure physical parameters for the interface to set it in Up status.

2.13.3 Default configurations of GARP

Default configurations of GARP are as below.

Function	Default value
GVRP status	Enable
GVRP registration mode	Normal
GARP Join timer	200ms

Function	Default value
GARP Leave timer	600ms
GARP LeaveAll timer	1000ms

2.13.4 Configuring GVRP

Configure GVRP for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`gvrp`** `{` **`enable`** `|` **`disable`** `}`	Enable/Disable global GVRP.
3	`Qtech(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
4	`Qtech(config-port)#` **`gvrp`** `{` **`enable`** `|` **`disable`** `}`	Enable/Disable interface GVRP.
5	`Qtech(config-port)#`**`gvrp registration`** `{` **`normal`** `|` **`fixed`** `|` **`forbidden`** `}`	Configure GVRP registration mode.
6	`Qtech(config-port)#`**`garp timer`** `{` **`join`**`|` **`leave`** `|` **`leaveall`** `}` *`timer`*	Configure the GARP timer.

2.13.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description

1	`Qtech#`**`show`** `{` **`garp`** `|` **`gvrp`** `}`
	`Qtech#`**`show`** `{` **`garp`** `|` **`gvrp`** `}` *`interface-type interface-number`*
	`Qtech#`**`show`** `{` **`garp`** `|` **`gvrp`** `}` *`interface-type interface-number`* **`statistics`**
		Show GARP/GVRP configurations or statistics.

2.13.6 Maintenance

Maintain the QSW-8200 series switch as below.

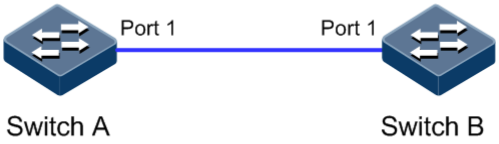
Command	Description
`Qtech(config)#`**`clear`** `{` **`garp`** `|` **`gvrp`** `}` *`interface-type interface-number`* **`statistics`**	Clear GARP/GVRP statistics on the interface.

2.13.7 Example for configuring GVRP

Networking requirements

As shown in Figure 2-24, to dynamically register and update VLAN configurations between switches, configure GVRP on these switches. Detailed requirements are as below:

Figure 2-24 GVRP networking



Configuration steps

Configurations of Switch A are the same with configurations of Switch. Take Switch A for example.

Step 1 Enable GVRP.

```
Qtech#hostname SwitchA
SwitchA#config
SwitchA(config)#gvrp enable
```

Step 2 Set port 1 to Trunk mode, and allow all VLANs to pass.

```
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport  mode trunk
SwitchA(config-port)#switchport trunk allowed vlan all
```

Step 3 Enable GVRP on port 1.

```
SwitchA(config-port)#gvrp enable
```

Checking results

Use the **show gvrp** command to show GVRP configurations.

Take Switch A for example.

```
SwitchA#show gvrp port 1
   Gvrp Globle Status:enable
   -----------------------------------------------------------------------
---
Port       PortStatus        RegMode
1           Enable            normal
```

3 IP services

This chapter describes basic principles and configurations of IP services, and provides related configuration examples, including the following sections:

- ARP
- Layer 3 interface
- Static routing

3.1 ARP

3.1.1 Introduction

In TCP/IP network environment, each host is assigned with a 32-bit IP address that is a logical address used to identify hosts between networks. To transmit packets in physical link, you must know the physical address of the destination host, which requires mapping the IP address to the physical address. In Ethernet environment, the physical address is a 48-bit MAC address. The system has to transfer the 32-bit IP address of the destination host to the 48-bit MAC address for transmitting packet to the destination host correctly. Then Address Resolution Protocol (ARP) is applied to resolve IP address to MAC address and set mapping between IP address and MAC address.

The ARP address table includes the following two types:

- Static entry: bind IP address and MAC address to avoid ARP dynamic learning cheating.
  - Static ARP address entry needs to be added/deleted manually.
  - No aging to static ARP address
- Dynamic entry: MAC address automatically learned through ARP
  - This dynamic entry is automatically generated by a switch. You can adjust partial parameters of it manually.
  - The dynamic ARP address entry will be aged after the aging time if not used.

3.1.2 Preparing for configurations

Scenario

The mapping of IP address and MAC address is saved in the ARP address table.

Generally, ARP address table is dynamically maintained by the QSW-8200 series switch. The QSW-8200 series switch searches for the mapping between IP address and MAC address automatically according to ARP. You just need to configure the QSW-8200 series switch manually for avoiding ARP dynamic learning cheating and adding static ARP address entries.

Prerequisite

N/A

3.1.3 Default configurations of ARP

Default configurations of ARP are as below.

Function	Default value
Static ARP entry	N/A
Aging time of dynamic ARP entries	1200s
Times of aging detection of dynamic ARP entries	3
Aging time of neighbor information entries	20min
Times of aging detection of neighbor information table entries	3

3.1.4 Configuring static ARP entries

Caution

- The IP address in static ARP entry must belong to the IP network segment of the Layer 3 interface of the device.
- The static ARP entry needs to be added and deleted manually.

Configure static ARP entries for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`arp`** *`ip-address mac-address`*	Configure static ARP entry.

3.1.5 Configuring ARP detection times

Configure static ARP detection times for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`arp detect-times`** *`time`*	Configure times for detecting aging of dynamic ARP entries.

3.1.6 Configuring aging time of ARP entries

Configure the aging time of ARP entries for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#arp aging-time` *`time`*	Configure the aging time of ARP entries.

3.1.7 Configuring times of aging detection of neighbor information table entries

Configure times of aging detection of neighbor information table entries for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#ipv6 nd aging-time` *`time`*	Configure the aging time of ARP entries.
3	`Qtech(config)#ipv6 nd detect-times` *`time`*	Configure times of aging detection of neighbor information table entries

3.1.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Qtech#show arp`	Show all information in ARP address table.
2	`Qtech#show arp` *`ip-address`*	Show the ARP entries related to specified IP address.
3	`Qtech#show arp` *`interface-type interface-number`*	Show the ARP entries related to the interface.
4	`Qtech#show arp static`	Show the static ARP entries.
5	`Qtech#show ipv6 neighbors`	Show information about the IPv6 neighbor mapping table.

3.1.9 Maintenance

Maintain the QSW-8200 series switch as below.

Command	Description
`Qtech(config)#clear arp`	Clear all entries in the ARP address table.

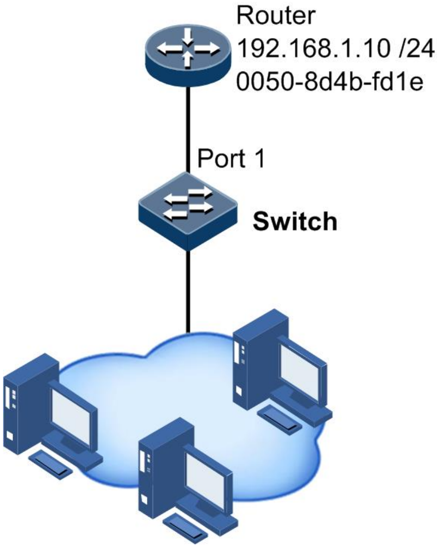
3.1.10 Example for configuring ARP

Networking requirements

As shown in Figure 3-1, the Switch connects to the host, and connects to upstream router through port 1. The IP address of the router is 192.168.1.10/24, and the MAC address is 0050-8d4b-fd1e.

You need to set the aging time of dynamic ARP entries to 600s. To improve communication security between the QSW-8200 series switch and router, you need to configure related static ARP entry on the Switch.

Figure 3-1 ARP networking



Configuration steps

Step 1 Create an ARP static entry.

```
Qtech(config)#arp 192.168.1.10 0050.8d4b.fd1e
```

Checking results

Use the **show arp** command to show all entries in the ARP address table.

```
Qtech#show arp
Ip Address        Mac Address          Type     Interface ip
```

```
----------------------------------------------------
192.168.1.10     0050.8d4b.fd1e      static    2
192.168.100.1    000F.E212.5CA0      dynamic    1

Total: 2
Static: 1
Dynamic: 1
```

3.2 Layer 3 interface

3.2.1 Introduction

The Layer 3 interface refers to the IP interface, and is a VLAN-based virtual interface. Configuring Layer 3 interface is generally used for device network management or routing link connection of multiple devices. Associating a Layer 3 interface with a VLAN requires configuring the IP address. Each Layer 3 interface corresponds to an IP address and is associated with at least one VLAN.

3.2.2 Preparing for configurations

Scenario

You can associate a Layer 3 interface with a VLAN when configuring the IP address for the Layer 3 interface. Each Layer 3 interface corresponds to an IP address and is associated with a VLAN.

Prerequisite

- Configure the VLAN associated with interfaces.
- Activate the VLAN.

3.2.3 Configuring Layer 3 interface

Configure the Layer 3 interface for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`interface ip`** *`if-number`*	Enter Layer 3 interface configuration mode.
3	`Qtech(config-ip)#`**`ip address`** *`ip-address`* `[` *`ip-mask`* `] [` **`sub`** `] [` *`vlan-list`* `]`	Configure the IP address for the Layer 3 interface, and associate it to the VLAN.
4	`Qtech(config-ip)#`**`ipv6 address`** *`ipv6-address/Prefix-length`*	(Optional) configure the IPv6 address of the Layer 3 interface.
4	`Qtech(config-ip)#`**`ip vlan`** *`vlan-list`*	Configure mapping between Layer 3 interface and VLAN.

Note

- Configure the VLAN associated with Layer 3 interface and activate it. You can use the command **state** { **active** | **suspend }** to activate the suspended VLAN before configuring it.
- Configure the VLAN associated with Layer 3 interface, and you can specify multiple VLANs at a time. If you configure the VLAN multiple times, the new configuration will override the original configuration, instead of accumulating with original configurations.
- The QSW-8200 series switch supports up to 15 Layer 3 interfaces, with the interface number ranging from 0 to 14.

3.2.4 Configuring IPv6 Layer 3 interface

Configure the IPv6 Layer 3 interface for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface ip** *if-number*	Enter Layer 3 interface configuration mode.
3	Qtech(config-ip)#**ipv6 address** *ipv6-address/Prefix-length*	Configure the IPv6 address for the Layer 3 interface.
4	Qtech(config-ip)#**ipv6 address** *ipv6-address* **link-local** *vlan-list*	Manually configure he IPv6 address for the Layer 3 interface, and associate it to the VLAN.
5	Qtech(config-ip)#**ipv6 address link-local** *vlan-list*	Automatically configure the IPv6 address for the Layer 3 interface, and associate it to the VLAN.

3.2.5 Checking configurations

Use the following commands to check configuration results.

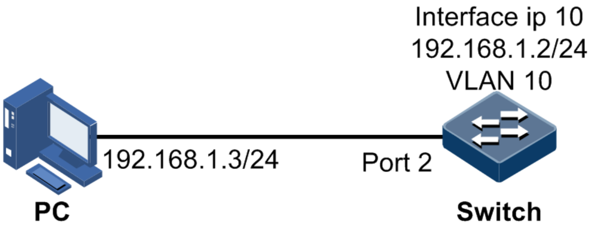
No.	Command	Description
1	Qtech#**show interface ip**	Show configurations of the IP address of the Layer 3 interface.
2	Qtech#**show interface ip vlan**	Show the binding between the Layer 3 interface and VLAN.
3	Qtech#**show interface ipv6**	Show configurations of the IPv6 address.

3.2.6 Example for configuring Layer 3 interface to interconnect with host

Networking requirements

As shown in Figure 3-2, configure the Layer 3 interface to interconnect the Switch so that the host and the Switch can ping through each other.

Figure 3-2 Layer 3 interface networking



Configuration steps

Step 1 Create a VLAN and add the interface into the VLAN.

```
Qtech#config
Qtech(config)#create vlan 10 active
Qtech(config)#interface port 2
Qtech(config-port)#switchport access vlan 10
```

Step 2 Configure Layer 3 interface on the QSW-8200 series switch, and configure the IP address, and associate the Layer 3 interface with the VLAN.

```
Qtech(config)#interface ip 10
Qtech(config-ip)#ip address 192.168.1.2 255.255.255.0 10
Qtech(config-ip)#exit
```

Checking results

Use the **show vlan** command to show association of VLAN and physical interface.

```
Qtech#show vlan 10
Switch Mode: --
VLAN Name          State   Status  Priority Member-Ports
-------------------------------------------------------------------------
10   VLAN0010      active  static  --       P2
```

Use the **show interface ip** command to show configurations of the Layer 3 interface.

```
Qtech#show interface ip
IF   Address        NetMask       Source     Catagory
----------------------------------------------------------
10   192.168.1.2   255.255.255.0  assigned    primary
```

Use the **show interface ip vlan** command to show association of Layer 3 interface and VLAN.

```
Qtech#show interface ip vlan
Ip Interface  Vlan list
----------------------------
0            1
…
10           10
…
```

Use the **ping** command to check whether the QSW-8200 series switch and PC can ping through each other.

```
Qtech#ping 192.168.1.3
Type CTRL+C to abort
Sending 5, 8-byte ICMP Echos to 192.168.18.119, timeout is 3 seconds:
Reply from 192.168.1.3: time<1ms
Reply from 192.168.1.3: time<1ms
Reply from 192.168.1.3: time<1ms
Reply from 192.168.1.3: time<1ms
Reply from 192.168.1.3: time<1ms

---- PING Statistics----
5 packets transmitted, 5 packets received,
Success rate is 100 percent(5/5),
round-trip (ms)  min/avg/max = 0/0/0.
```

3.3 Static routing

3.3.1 Introduction

Routing is required for communication among different devices in one VLAN, or different VLANs. Routing is to transmit packets through network to destination, which adopts routing table for forwarding packets.

There are three modes to execute routing function:

- Default routing: forwarding the packets without destination address to an assigned default router.
- Static routing: configure routing manually to forward packets from the assigned interface. This is suitable to simple network topology.

- Dynamic routing: learning routing dynamically through routing protocol which can calculate the best route for packets forwarding. This mode will take up more bandwidth and network resource. Now, there are two dynamic routing protocols available:
  - Distance vector protocol: each device maintains a vector table, which lists the known best distance and path to other destination devices. By exchanging information with neighbor devices, the QSW-8200 series switch can update internal vector table continuously.
  - Link status protocol: the QSW-8200 series switch builds link status database through network interface status notification; the database contains status of all links straight-connected to all devices. All devices share the same network topology, but each device can judge the best path to each node in network topology. Link status protocol can respond on topology changes quickly, but need more bandwidth and resources compared with distance vector protocol.

The QSW-8200 series switch supports default routing and static routing only but dynamic routing.

Default routing

Default routing is a special routing that only be used when there is no matched item in the routing table. Default routing appears as a route to network 0.0.0.0 (with mask 0.0.0.0) in the routing table. You can show default routing configuration by using the **show ip route** command. If the destination address of a packet cannot match with any item in the routing table, the packet will choose default routing. If the QSW-8200 series switch has not been configured with default routing and the destination IP of the packet is not in the routing table, the QSW-8200 series switch will discard the packet and return an ICMP packet to the Tx end to inform that the destination address or network is unavailable.

Static routing

Static routing is routing configured manually. It is available to simple, small, and stable network. The disadvantage is that it cannot adapt to network topology changes automatically and needs manual intervention.

3.3.2 Preparing for configurations

Scenario

Configure static routing for simple network topology manually to build an intercommunication network.

Prerequisite

Configure the IP address for Layer 3 interface correctly.

3.3.3 Configuring default gateway

Note

When a packet to be forwarded does not have the correspoding route on the QSW-8200 series switch, use the **ip default-gateway** command to configure default gateway, and forward this packet to default gateway. The IP address of default gateway must be in the same network segment with the IP address of any local IP interface.

Configure default gateway on the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**ip default-gateway** *ip-address*	Configure the IPv4 address of the default gateway.
3	Qtech(config)#**ipv6 default-gateway** *ipv6-address*	Configure the IPv6 address of the default gateway.

3.3.4 Configuring static routing

Configure static routing for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**ip route** *ip-address* { *masklength* | *ip-mask* } *next-hop-ip-address*	Configure static route based on IPv4.
3	Qtech(config)#**ipv6 route** *ip-address masklength next-hop-ip-address*	Configure static route based on IPv6.

3.3.5 Checking configurations

Use the following commands to check configuration results.

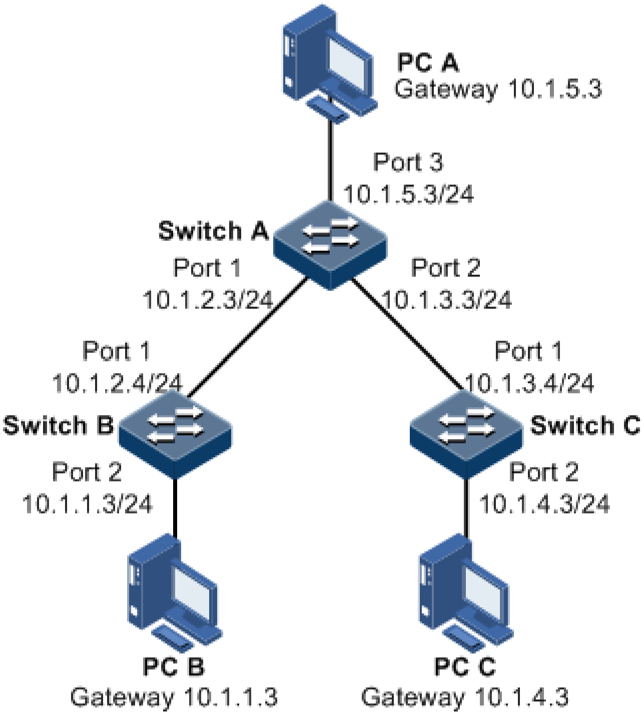
No.	Item	Description
1	Qtech#**show ip route**	Show device routing table information.
2	Qtech#**show ipv6 route** [**detail**]	Show information about the IPv6 routing table.
3	Qtech#**show ip route detail**	Show details about the routing table.

3.3.6 Example for configuring static routing

Networking requirements

Configure static routing to enable any two hosts or QSW-8200 series switch devices successfully ping through each other, as shown in Figure 3-3.

Figure 3-3 Configuring static routing



Configuration steps

Step 1 Configure the IP address of each device. Detailed configurations are omitted.

Step 2 Enable routing and configure static routing on Switch A.

```
Qtech#hostname SwitchA
SwitchA#config
SwitchA(config)#ip route 10.1.1.0 255.255.255.0 10.1.2.4
SwitchA(config)#ip route 10.1.4.0 255.255.255.0 10.1.3.4
```

Step 3 Enable routing and configure the default gateway on Switch B.

```
Qtech#hostname SwitchB
SwitchB(config)#ip default-gateway 10.1.2.3
```

Step 4 Enable routing and configure the default gateway on Switch C.

```
Qtech#hostname SwitchC
SwitchC(config)#ip default-gateway 10.1.3.3
```

Step 5 Set the default gateway of host A to 10.1.5.3. Detailed configurations are omitted.

Set the default gateway of host B to 10.1.1.3. Detailed configurations are omitted.

Set the default gateway of host C to 10.1.4.3. Detailed configurations are omitted.

Checking results

Use the **ping** command to check whether any two of all devices can ping through each other.

```
SwitchA#ping 10.1.1.3
Type CTRL+C to abort
Sending 5, 8-byte ICMP Echos to 10.1.1.3, timeout is 3 seconds:
Reply from 10.1.1.3: time<1ms
Reply from 10.1.1.3: time<1ms
Reply from 10.1.1.3: time<1ms
Reply from 10.1.1.3: time<1ms
Reply from 10.1.1.3: time<1ms

---- PING Statistics----
5 packets transmitted, 5 packets received,
Success rate is 100 percent(5/5),
round-trip (ms)  min/avg/max = 0/0/0.
```

4 DHCP

This chapter describes basic principle and configuration procedure for DHCP, and provides related configuration example, including the following sections:

- DHCP Server
- DHCP Client
- DHCP Relay
- DHCP Snooping
- DHCP Option

4.1 DHCP Server

4.1.1 Introduction

Dynamic Host Configuration Protocol (DHCP) refers to assign IP address configurations dynamically for users in TCP/IP network. It is based on BOOTP (Bootstrap Protocol) protocol, and automatically adds the specified available network address, network address re-use, and other extended configuration options over BOOTP protocol.

With enlargement of network scale and development of network complexity, the number of PCs on a network usually exceeds the maximum number of distributable IP addresses. Meanwhile, the widely use of notebooks and wireless networks lead to frequent change of PC positions and also related IP addresses must be updated frequently. As a result, network configurations become more and more complex. DHCP is developed to solve these problems.

DHCP adopts client/server communication mode. A client applies configuration to the server (including IP address, Subnet mask, and default gateway), and the server replies with IP address for the client and other related configurations to implement dynamic configurations of IP address, etc.

In DHCP Client/Server communication mode, a specific host is configured to assign IP addresses, and send network configurations to related hosts. The host is called the DHCP server.

DHCP application

Under normal circumstances, use the DHCP server to assign IP addresses in following situations:

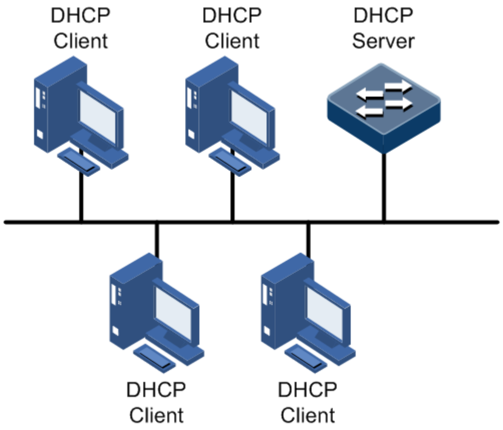
- The network scale is large. It requires much workload for manual configurations, and is difficult to manage the entire network intensively.
- The number of hosts on the network is greater than the number of IP addresses, which make it unable to assign a fixed IP address for each host, and restrict the number of users connected to network simultaneously.
- Only the minority of hosts on the network need fixed IP addresses, most of hosts have no requirement for fixed IP address.

After a DHCP client obtains the IP address from the DHCP server, it cannot use the IP address permanently but in a fixed period, which is called the leased period. You can specify the duration of the leased period.

The DHCP technology ensures rational allocation, avoids waste of IP addresses, and improves the utilization rate of IP addresses on the entire network.

The QSW-8200 series switch, as the DHCP server, assigns dynamic IP addresses to clients, as shown in Figure 4-1.

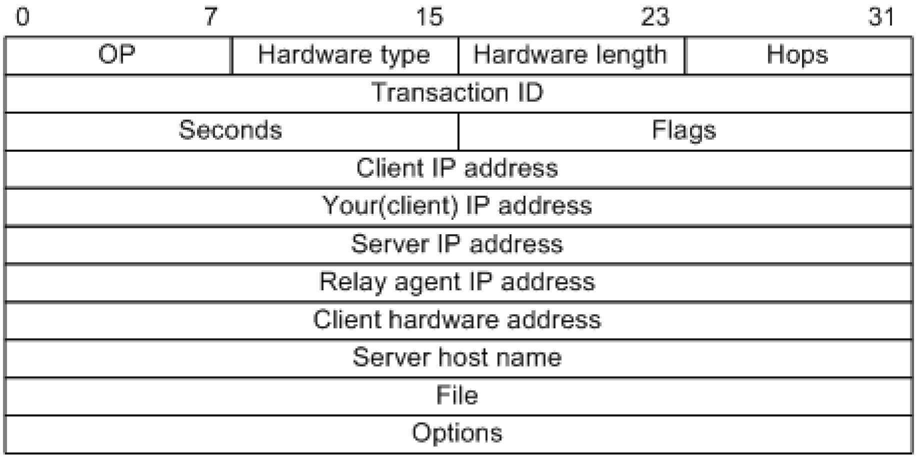
Figure 4-1 DHCP Server and Client networking



DHCP packets

Figure 4-2 shows the structure of a DHCP packet. The DHCP packet is encapsulated in a UDP data packet.

Figure 4-2 Structure of a DHCP packet



OP	Hardware type	Hardware length	Hops
Transaction ID			
Seconds		Flags	
Client IP address			
Your(client) IP address			
Server IP address			
Relay agent IP address			
Client hardware address			
Server host name			
File			
Options			

Table 4-1 describes fields of a DHCP packet.

Table 4-1 Fields of a DHCP packet

Field	Length	Description
OP	1	Packet type ● 1: a request packet ● 2: a reply packet
Hardware type	1	Hardware address type of a DHCP client
Hardware length	1	Hardware address length of a DHCP client
Hops	1	Number of DHCP hops passing by the DHCP packet This field increases 1 every time the DHCP request packet passes a DHCP relay.
Transaction ID	4	A random number selected by the client to initiate a request, used to identify an address request process
Seconds	2	Duration after the DHCP request for the DHCP client, fixed to 0, being idle currently
Flags	2	Bit 1 is the broadcast reply flag, used to mark that the DHCP server response packet is transmitted in unicast or broadcast mode. ● 0: unicast ● 1: broadcast Other bits are reserved.
Client IP address	4	IP address of the DHCP client, only filled when the client is in bound, updated or re-bound status, used to respond to ARP request
Your (client) IP address	4	IP address of the DHCP client assigned by the DHCP server
Server IP address	4	IP address of the DHCP server
Relay agent IP address	4	IP address of the first DHCP relay passing by the request packet sent by the DHCP client
Client hardware address	16	Hardware address of the DHCP client
Server host name	64	Name of the DHCP server
File	128	Startup configuration file name and path assigned by the DHCP server to the DHCP client
Options	Modifiable	A modifiable option field, including packet type, available leased period, IP address of the Domain Name System (DNS) server, IP address of the Windows Internet Name Server (WINS), etc.

4.1.2 Preparing for configurations

Scenario

DHCP adopts client/server mode, so the DHCP server can automatically assign IP addresses and transmit network parameters for clients.

Prerequisite

DHCP Server/Client is mutually exclusive to DHCP Snooping/Replay. Namely, you cannot configure them concurrently on a device. DHCP Relay and DHCP Snooping can be enabled on the same device.

4.1.3 Default configurations of DHCP Server

Default configurations of DHCP Server are as below.

Function	Default value
Global DHCP Server	Disable
Global DHCPv6 Server status	Disable
IP port DHCP Server	Disable
Layer 3 interface DHCPv6 Server status	Disable
Address pool	N/A
Global leased period	• Maximum leased period: 10080 minutes • Minimum leased period: 30 minutes • Default leased period: 30 minutes
Address pool leased period	• Maximum leased period: 0 minutes • Minimum leased period: 0 minutes • Default leased period: 0 minutes
Trusted relay address	N/A

4.1.4 Configuring global DHCP Server

Configure global DHCP Server for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`ip dhcp server`**	Enable global DHCP Server.
3	`Qtech(config)#`**`ip dhcp server default -lease`** `{` *`minute`* `|` **`infinite`** `}`	(Optional) configure global default leased period.
4	`Qtech(config)#`**`ip dhcp server min-lease`** `{` *`minute`* `|` **`infinite`** `}`	(Optional) configure global minimum leased period. The value **infinite** indicates an infinite leased period.

Step	Command	Description
5	`Qtech(config)#ip dhcp server max-lease { minute | infinite }`	(Optional) configure global maximum leased period. The value **infinite** indicates an infinite leased period.

4.1.5 Enabling global DHCPv6 Server

Enable global DHCPv6 Server for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#ipv6 dhcp server`	Enable global DHCPv6 Server.

4.1.6 Configuring address pool

To enable the DHCP server to assign IP addresses and network parameters for clients, you must create an address pool on the DHCP server.

Configure the address pool for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#ip dhcp server pool pool-name`	Create an address pool, and enter address pool mode.
3	`Qtech(dhcp-pool)#address start-ip-address end-ip-address mask { ip-mask | mask-length }`	Configure the range of IP addresses and mask of the address pool.
4	`Qtech(dhcp-pool)#lease default { minute | infinite } [ min { minute | infinite } ] [ max { minute | infinite } ]`	(Optional) configure the default, minimum, maximum leased period for the address pool. The value **infinite** indicates an infinite leased period. Use the **no lease config** command to restore the default value.
5	`Qtech(dhcp-pool)#dns-server ip-address`	(Optional) configure the DNS server address of the address pool.
	`Qtech(dhcp-pool)#dns-server secondary ip-address`	(Optional) configure the IP address of the secondary DNS server of the address pool.
6	`Qtech(dhcp-pool)#gateway ip-address`	(Optional) configure the default gateway of the address pool.
7	`Qtech(dhcp-pool)#tftp-server ip-address`	(Optional) configure the TFTP server address of the address pool.

Step	Command	Description
	Qtech(dhcp-pool)#**bootfile** *file-name*	(Optional) configure the boot file name of the address pool.

4.1.7 Configuring IPv6 address pool

To enable the DHCPv6 server to assign IPv6 addresses and network parameters for clients, you must create an address pool on the DHCPv6 server.

Configure the IPv6 address pool for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**ipv6 dhcp server pool** *pool-name*	Create an IPv6 address pool, and enter address pool mode.
3	Qtech(dhcp-pool)#**address prefix** *ipv6-address/prefix-length*	Configure the prefix of the IPv6 address pool.
4	Qtech(dhcp-pool)#**lifetime preferred-lifetime** { *minute* | **infinite** } **valid-lifetime**{ *minute* | **infinite** }	(Optional) configure timers of the IPv6 address pool, including the preferred lifetime and valid lifetime.
5	Qtech(dhcp-pool)#**dns-server** *ipv6-address*	(Optional) configure the IP address of the DNS server for the IPv6 address pool.

4.1.8 Configuring DHCP Server on IP interface

Only when DHCP Server is enabled both globally and on IP interfaces and the address pool is bound to the IP interface, can the IP interface receives and processes DHCP request packets from clients.

Configure DHCP Server on the IP interface for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface ip** *if-number*	Enter Layer 3 interface configuration mode.
3	Qtech(config-ip)#**ip dhcp server**	Enable DHCP Server on the IP interface.
4	Qtech(config-ip)#**ip address** *ip-address*	Configure the IP address of the interface.

Step	Command	Description
5	`Qtech(config-ip)#ip vlan vlan-id`	Configure VLAN related to the IP interface. Note If the IP interface is not related to any VLAN, create a VLAN and make them associated.
6	`Qtech(config-ip)#ip dhcp server pool pool-name`	Bind the address pool to the IP interface.

Note

- After an address pool is bound to an interface, its parameters cannot be modified. If you have to modify its parameters, unbind it in advance.
- An address pool can be bound to only one IP interface; however, an IP interface can be related to up to 5 address pools.

4.1.9 Configuring DHCPv6 Server on IP interface

Only when DHCP Server is enabled both globally and on IP interfaces and the address pool is bound to the IP interface, can the IP interface receives and processes DHCP request packets from clients.

Configure DHCP Server on the IP interface for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#interface ip if-number`	Enter Layer 3 interface configuration mode.
3	`Qtech(config-ip)#ipv6 dhcp server`	Enable DHCPv6 Server on the IP interface.
4	`Qtech(config-ip)#ipv6 dhcp server rapid-commit`	(Optional) enable rapid interaction on the IPv6 interface.
5	`Qtech(config-ip)#ipv6 address ipv6-address/Prefix-length`	Configure the IPv6 address of the interface.
6	`Qtech(config-ip)#ip vlan vlan-id`	Configure the VLAN associated with the IP interface.
7	`Qtech(config-ip)#ipv6 dhcp server pool pool-name`	Bind the IPv6 address pool to the IPv6 address.

4.1.10 (Optional) configuring trusted DHCP relay

When DHCP clients and the server are in different network segments, a DHCP relay is required to forward DHCP packets. Under this situation, you need to configure the IP address of the trusted DHCP relay on the DHCP server.

Configure the trusted DHCP relay for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#ip dhcp server relay-ip` *`ip-address`* `{` *`ip-mask`* `|` *`mask-length`* `}`	Configure the IP address of the trusted DHCP relay.

4.1.11 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Qtech#show ip dhcp server`	Show configurations of DHCP Server.
2	`Qtech#show ip dhcp server pool [` *`pool-name`* `]`	Show configurations of the address pool of DHCP Server.
3	`Qtech#show ip dhcp server relay-ip`	Show information about the relay trusted by the DHCP server.
4	`Qtech#show ip dhcp server lease`	Show assigned IP addresses and clients information.
5	`Qtech#show ip dhcp server statistics`	Show packet statistics of DHCP Server.
6	`Qtech#show ipv6 dhcp server`	Show configurations of global and interface DHCPv6 Server.
7	`Qtech#show ipv6 dhcp server pool [` *`pool-name`* `]`	Show configurations of the IPv6 address pool of DHCPv6 Server.
8	`Qtech#show ipv6 dhcp server binding`	Show assigned IPv6 addresses and their clients' information.

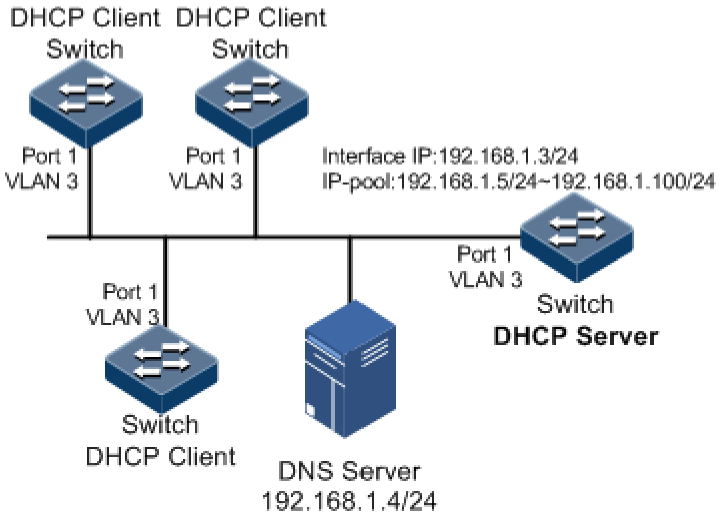
4.1.12 Example for configuring DHCP Server and DHCP Client

Networking requirements

As shown in Figure 4-3, Switch A, as the DHCP server, assigns dynamic IP addresses for clients on the same network.

By configuring dynamic assignment of IP addresses, you can reduce manual configuration workload and improve the utilization rate of IP addresses.

Figure 4-3 DHCP Server networking



Configuration steps

Step 1 Configure the interface that connects to the DHCP client.

```
Qtech#config
Qtech(config)#create vlan 3 active
Qtech(config)#interface port 1
Qtech(config-port)#switchport access vlan 3
Qtech(config-port)#exit
```

Step 2 Enable global DHCP Server.

```
Qtech(config)#ip dhcp server
```

Step 3 Configure the address pool of DHCP Server.

```
Qtech(config)#ip dhcp server pool Qtech1
Qtech(dhcp-pool)#address 192.168.1.5 192.168.1.100 mask 24
Qtech(dhcp-pool)#dns-server 192.168.1.4
Qtech(dhcp-pool)#exit
```

Step 4 Configure DHCP Server on the IP interface.

```
Qtech(config)#interface ip 0
Qtech(config-ip)#ip dhcp server
Qtech(config-ip)#ip dhcp server pool Qtech1
Qtech(config-ip)#ip address 192.168.1.3 3
```

Configure DHCP clients. Each DHCP client has the same configurations, so take one for example.

Step 5 Configure the interface that connects to the DHCP server.

```
Qtech#config
Qtech(config)#create vlan 3 active
Qtech(config)#interface port 1
Qtech(config-port)#switchport access vlan 3
Qtech(config-port)#exit
```

Step 6 Configure the DHCP client to apply for IP address through DHCP.

```
Qtech#config
Qtech(config)#interface ip 0
Qtech(config-ip)#ip vlan 3
Qtech(config-ip)#ip address dhcp server-ip 192.168.1.3
```

Checking results

Check the DHCP server as below:

Use the **show ip dhcp server** command to show configurations of DHCP Server.

```
Qtech#show ip dhcp server
Global DHCP Server:  Enable
Global Minimum Lease: 30   minutes
Global Default Lease: 30   minutes
Global Maximum Lease: 10080minutes

Interface     Status       Pools bind
-------------------------------------------
 IP0         Enable       Qtech1
 IP1         Disable       --
 IP2        Disable       --
 IP3         Disable       --
 ……
 IP13        Disable       --
  IP14        Disable       --
```

Use the **show ip dhcp server pool** [*pool-name*] command to show configurations of the address pool of DHCP Server.

```
Qtech#show ip dhcp server pool Qtech1
Pool Name:          Qtech1
Associated Interface: IP0
```

```
Address Range:      192.168.1.5~192.168.1.100
Address Mask:       255.255.255.0
Gateway:            0.0.0.0
DNS Server:         192.168.1.4
Secondary DNS:      0.0.0.0
Tftp Server:        0.0.0.0
Bootfile:           --
Default Lease:      0    minutes
Minimum Lease:      0    minutes
Maximum Lease:      0    minutes
```

Check the DHCP client as below:

Use the **show ip dhcp client** command to show configurations of DHCP Client.

```
Qtech#show ip dhcp client
  Hostname:                Qtech
  Class-ID:                Qtech-ROS
  Client-ID:               Qtech-001fce000010-IF0
  Assigned IP Addr:         192.168.1.5
  Subnet mask:             255.255.255.0
  Default Gateway:          --
  Client lease Starts:      Jan-01-2010 08:58:10
  Client lease Ends:        Jan-01-2010 09:28:10
  Client lease duration:    1800(sec)
  DHCP Server:             192.168.1.3
  Tftp server name:         --
  Tftp server IP Addr:      --
  Startup_config filename:   --
  NTP server IP Addr:       --
  Root path:               --
```

Use the **show interface ip** command to check whether the DHCP client has obtained the IP address.

```
Qtech#show interface ip
IF   Address       NetMask       Source     Catagory
----------------------------------------------------------
0    192.168.1.5   255.255.255.0  dhcp       primary
```

4.2 DHCP Client

4.2.1 Introduction

The QSW-8200 series switch supports working as a DHCP client and obtaining the IP address from the DHCP server so that it can be managed later.

4.2.2 Preparing for configurations

Scenario

The QSW-8200 series switch supports working as a DHCP client and obtaining the IP address from the DHCP server so that it can be managed later.

The IP address assigned to the DHCP client is limited with a certain leased period in dynamic address distribution mode. The DHCP server takes back the IP address when it expires. Then, the DHCP client has to re-lease IP address for continuous using. The DHCP client can release IP address if it does not want to use it any more before its expiration.

We recommend that the number of DHCP relays be smaller than 4 if the DHCP client needs to obtain the IP address from the DHCP server through multiple DHCP relays.

Prerequisite

- DHCP Server/Client is mutually exclusive to DHCP Snooping/Replay. Namely, you cannot configure them concurrently on a device. DHCP Relay and DHCP Snooping can be enabled on the same device.
- Create a VLAN, and add the Layer 3 interface to it.
- A DHCP server is ready.

4.2.3 Default configurations of DHCP Client

Default configurations of DHCP Client are as below.

Function	Default value
hostname	Qtech
class-id	Qtech-ROS
client-id	Qtech-SYSMAC-IF0
DHCPv6 Client	Disable
DHCPv6 Client relet	Automatical
DHCPv6 Client application rapid interaction	Disable

4.2.4 Configuring DHCP Client

Only interface IP 0 on the Switch supports DHCP Client.

For interface IP 0, the IP address obtained through DHCP and the one configured manually can overwrite each other.

Configure the DHCP client for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.

Step	Command	Description
2	Qtech(config)#**interface ip 0**	Enter Layer 3 interface configuration mode.
3	Qtech(config-ip)#**ip vlan** *vlan-id*	Configure applying for an IP address through DHCP.
4	Qtech(config-ip)#**ip dhcp client** { **class-id** *class-id* | **client-id** *client-id* | **hostname** *hostname* }	(Optional) configure the DHCP client, including class ID, client ID, and host name. ⚠ Caution After the DHCP client obtains the IP address through DHCP, its information cannot be modified.
5	Qtech(config-ip)#**ip address dhcp** [**server-ip** *ip-address*]	Configure the QSW-8200 series switch to apply for the IP address through DHCP. If the QSW-8200 series switch has obtained an IP address from the DHCP server through DHCP before, it will restart the application process for the IP address if you use the **ip address dhcp** command to modify the IP address of the DHCP server.
6	Qtech(config-ip)#**ip dhcp client renew**	(Optional) renew the IP address. If the Layer 3 interface of the QSW-8200 series switch has obtained an IP address through DHCP, the IP address will automatically be renewed when the leased period expires.
7	Qtech(config-ip)#**no ip address dhcp**	(Optional) release the IP address, and shut down the DHCP client.

4.2.5 Configuring DHCPv6 Client

Only interface IP 0 on the Switch supports DHCPv6 Client.

For interface IP 0, the IP address obtained through DHCP and the one configured can manually overwrite each other.

Configure the DHCPv6 client for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface ip 0**	Enter Layer 3 interface configuration mode.

Step	Command	Description
3	`Qtech(config-ip)#ip vlan vlan-id`	Configure the VLAN associated with the IP interface. If the VLAN to be associated does not exist, create it, and then associate it with the IP interface.
4	`Qtech(config-ip)#ipv6 address dhcp [ server-ip ipv6-address ]`	Configure applying for IPv6 address through DHCPv6. If the QSW-8200 series switch has obtained an IP address from the DHCP server through DHCPv6 before, it will restart the application process for the IP address if you use the command to modify the IPv6 address of the DHCP server.
5	`Qtech(config-ip)#ipv6 dhcp client renew`	(Optional) renew the IPv6 address. If the Layer 3 interface of the QSW-8200 series switch has obtained an IP address through DHCP, the IPv6 address will automatically be renewed when the leased period expires.
6	`Qtech(config-ip)# ipv6 dhcp client rapid-commit`	(Optional) enable DHCP6 Client to apply for rapid interaction.

4.2.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Qtech#show ip dhcp client`	Show configurations of the DHCP client.
2	`Qtech#show ipv6 dhcp client`	Show configurations of the DHCPv6 client.

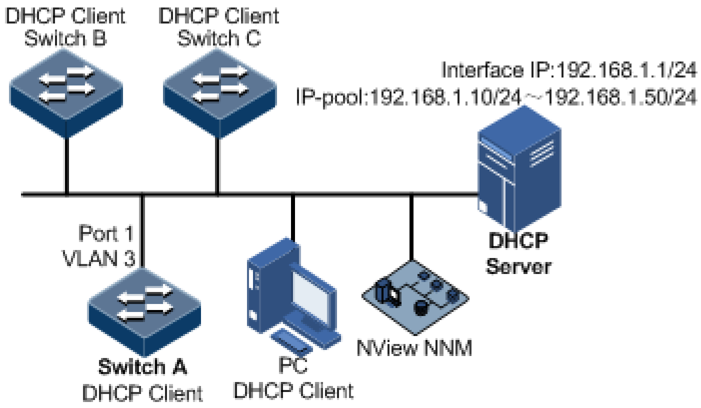
4.2.7 Example for configuring DHCP Client

Networking requirements

As shown in Figure 4-4, multiple DHCP clients in a VLAN are connected to the DHCP server and the NMS.

Configure the DHCP server to assign an IP address to the Switch and make the NMS manage the Switch.

Figure 4-4 DHCP client networking



Configuration steps

Each DHCP client has the same configurations. Take Switch A for example.

DHCP Server should be configured in advance. Its configurations are omitted here.

Step 1 Configure attributes of the interface connected to the DHCP server.

```
Qtech#config
Qtech(config)#create vlan 3 active
Qtech(config)#interface port 1
Qtech(config-port)#switchport access vlan 3
Qtech(config-port)#exit
```

Step 2 Configure the DHCP client to apply for the IP address through DHCP.

```
Qtech#config
Qtech(config)#interface ip 0
Qtech(config-ip)#ip vlan 3
Qtech(config-ip)#ip dhcp client hostname Qtech
Qtech(config-ip)#ip address dhcp server-ip 192.168.1.1
```

Checking results

Use the **show ip dhcp client** command to show configurations of DHCP Client.

```
Qtech#show ip dhcp client
  Hostname:                Qtech
  Class-ID:                Qtech-ROS
  Client-ID:               Qtech-001fce000010-IF0
  Assigned IP Addr:         192.168.1.10
  Subnet mask:              255.255.255.0
  Default Gateway:           --
```

```
Client lease Starts:      Jan-01-2010 08:07:01
Client lease Ends:        Jan-01-2010 08:37:01
Client lease duration:    1800(sec)
DHCP Server:              192.168.1.1
Tftp server name:         --
Tftp server IP Addr:       --
Startup_config filename:   --
NTP server IP Addr:        --
Root path:                 --
```

Use the **show interface ip** command to check whether the DHCP client has obtained the IP address.

```
Qtech#show interface ip
IF   Address       NetMask        Source     Catagory
----------------------------------------------------------
0    192.168.1.10   255.255.255.0   dhcp       primary
```

4.3 DHCP Relay

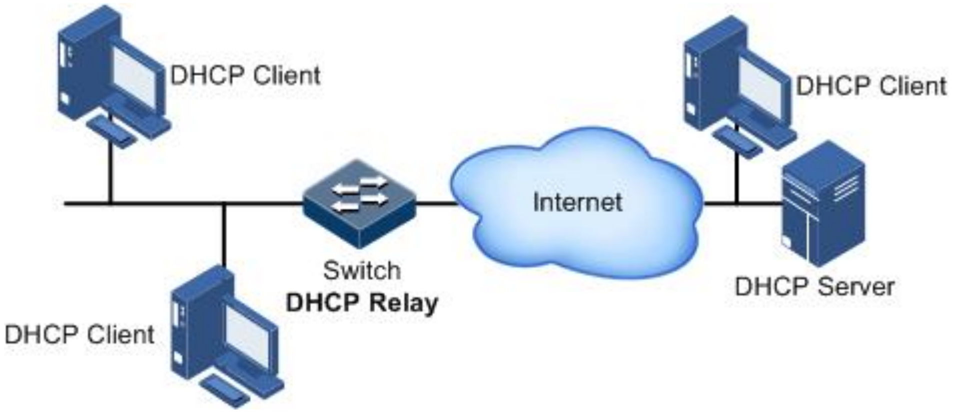
4.3.1 Introduction

At the beginning, DHCP requires the DHCP server and clients to be in the same network segment, instead of different network segments. As a result, a DHCP server is configured for all network segments for dynamic host configuration, which is not economic.

DHCP Relay is introduced to solve this problem. It can provide relay service between DHCP clients and DHCP server that are in different network segments. It relays packets across network segments to the DHCP server or clients.

Figure 4-5 shows typical application of DHCP Relay. DHCP clients in different network segments can share the same DHCP server, thus saving costs.

Figure 4-5 Typical application of DHCP Relay



4.3.2 Preparing for configurations

Scenario

When DHCP Client and DHCP Server are not in the same network segment, you can use DHCP Relay function to make DHCP Client and DHCP Server in different network segments carry relay service, and relay DHCP protocol packets across network segment to destination DHCP server, so that DHCP Client in different network segments can share the same DHCP server.

Prerequisite

DHCP Server/Client is mutually exclusive to DHCP Snooping/Replay. Namely, you cannot configure them concurrently on a device. DHCP Relay and DHCP Snooping can be enabled concurrently.

4.3.3 Default configurations of DHCP Relay

Default configurations of DHCP Relay are as below.

Function	Default value
Global DHCP Relay	Disable
DHCP Relay on the Layer 3 interface	Enable
Global DHCPv6 Relay status	Disable
Layer 3 interface DHCPv6 Relay status	Disable
DHCP Relay supporting Option 82	Disable
Policy for DHCP Relay to process Option 82 request packets	Replace

4.3.4 Configuring global DHCP Relay

Configure global DHCP Relay for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#ip dhcp relay`	Enable global DHCP Relay.

4.3.5 Configuring global DHCPv6 Relay

Configure global DHCPv6 Relay for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.

Step	Command	Description
2	`Qtech(config)#ipv6 dhcp relay`	Enable global DHCPv6 Relay.

4.3.6 Configuring DHCP Relay on IP interface

Configure DHCP Relay on the IP interface for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#interface ip if-number`	Enter Layer 3 interface configuration mode.
3	`Qtech(config-ip)#ip dhcp relay`	Enable DHCP Relay on the IP interface.

4.3.7 Configuring DHCPv6 Relay on IP interface

Configure DHCPv6 Relay on the IP interface for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#interface ip if-number`	Enter Layer 3 interface configuration mode.
3	`Qtech(config-ip)#ipv6 dhcp relay`	Enable DHCPv6 Relay on the IPv6 interface.

4.3.8 Configuring destination IP address for forwarding packets

Configure the destination IP address for forwarding packets for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#interface ip if-number`	Enter Layer 3 interface configuration mode.
3	`Qtech(config-ip)#ip dhcp relay`	Enable DHCP Relay on the IP interface.
4	`Qtech(config-ip)#ip dhcp realy target-ip ip-address`	Configure the destination IP address (IP address of the DHCP server or that of the next hop DHCP relay) for forwarding packets.

4.3.9 Configuring destination IPv6 address for forwarding packets

Configure the destination IPv6 address for forwarding packets for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`interface ip`** *`if-number`*	Enter Layer 3 interface configuration mode.
3	`Qtech(config-ip)#`**`ipv6 dhcp relay`**	Enable DHCPv6 Relay on the IPv6 interface.
4	`Qtech(config-ip)#`**`ipv6 dhcp relay target-ip`** *`ipv6-address`*[**ip** *if-number*]	Configure the destination IP address (IP address of the DHCP server or egress interface) for forwarding packets.

4.3.10 (Optional) configuring DHCP Relay to support Option 82

Configure DHCP Relay to support Option 82 for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`ip dhcp relay information option`**	Configure DHCP Relay to support Option 82.
3	`Qtech(config)#`**`ip dhcp relay information policy`** `{` **`drop`** `|` **`keep`** `|` **`replace`** `}`	Configure the policy for DHCP Relay to process Option 82 request packets

4.3.11 Checking configurations

Use the following commands to check configuration results.

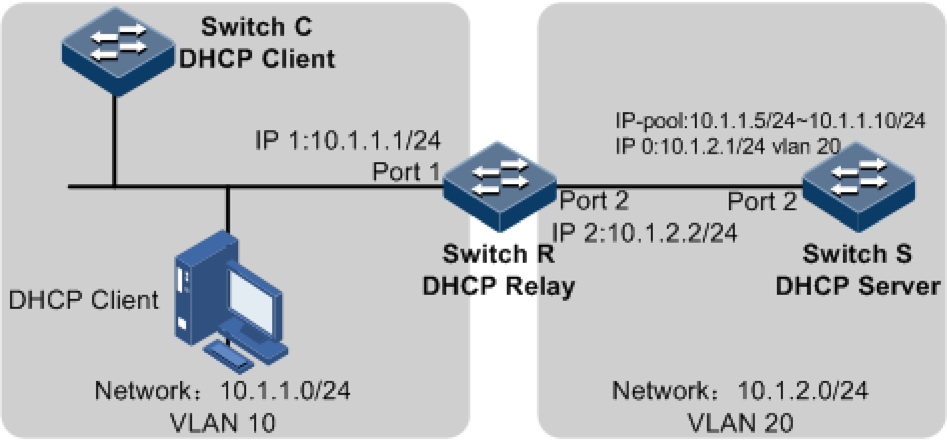
No.	Command	Description
1	`Qtech#`**`show ip dhcp relay`**	Show configurations or statistics of DHCP Relay.
2	`Qtech#`**`show ip dhcp relay information`**	Show configurations of DHCP Replay to support Option 82.
3	`Qtech#`**`show ipv6 dhcp relay`**	Show configurations of DHCPv6 Relay.

4.3.12 Example for configuring DHCP Relay and DHCP Server

Networking requirements

As shown in Figure 4-6, the DHCP client and DHCP server are in different network segments. If the DHCP client needs to apply for the IP address from the DHCP server, the application has to pass the DHCP relay.

Figure 4-6 DHCP Relay networking



Configuration steps

Configure the DHCP relay Switch R.

Step 1 Configure the interface attributes.

```
Qtech#config
Qtech(config)#create vlan 10,20 active
Qtech(config)#interface port 1
Qtech(config-port)#switchport access vlan 10
Qtech(config-port)#exit
Qtech(config)#interface port 2
Qtech(config-port)#switchport access vlan 20
Qtech(config-port)#exit
Qtech(config)#interface ip 1
Qtech(config-ip)ip address 10.1.1.1 255.255.255.0 10
Qtech(config-ip)#exit
Qtech(config)#interface ip 2
Qtech(config-ip)ip address 10.1.2.2 255.255.255.0 20
Qtech(config-ip)#exit
```

Step 2 Enable global DHCP Relay and DHCP Relay on the IP interface.

```
Qtech(config)#ip dhcp relay
Qtech(config)#interface ip 1
Qtech(config-ip)#ip dhcp relay
```

Step 3 Configure the destination IP address for forwarding packets.

```
Qtech(config-ip)#ip dhcp realy target-ip 10.1.2.1
Qtech(config-ip)#exit
```

Configure the DHCP server Switch S.

Step 4 Configure the interface.

```
Qtech(config)#create vlan 20 active
Qtech(config)#interface port 2
Qtech(config-port)#switchport access vlan 20
Qtech(config-port)#exit
```

Step 5 Enable global DHCP Server.

```
Qtech(config)#ip dhcp server
```

Step 6 Configure the address pool of the DHCP server.

```
Qtech(config)#ip dhcp server pool Qtech1
Qtech(dhcp-pool)#address 10.1.1.5 10.1.1.10 mask 24
Qtech(dhcp-pool)#gateway 10.1.1.1
Qtech(dhcp-pool)#dns-server 10.1.1.4
Qtech(dhcp-pool)#exit
```

Step 7 Enable DHCP Server on the IP interface.

```
Qtech(config)#interface ip 0
Qtech(config-ip)#ip dhcp server
Qtech(config-ip)#ip dhcp server pool Qtech1
Qtech(config-ip)#ip address 10.1.2.1 255.255.255.0 20
Qtech(config-ip)#exit
```

Step 8 Configure trusted DHCP Relay.

```
Qtech(config)#ip dhcp server relay-ip 10.1.1.1 24
```

Step 9 Configure routes.

```
Qtech(config)#ip route 10.1.1.0 255.255.255.0 10.1.2.2
```

Configure the DHCP client Switch C.

Step 10 Configure the DHCP client to apply for the IP address through DHCP.

```
Qtech(config)#interface ip 0
Qtech(config-ip)#ip vlan 1
Qtech(config-ip)#ip address dhcp
```

Checking results

Check the DHCP relay.

Use the following command to show configurations of DHCP Relay.

```
Qtech#show ip dhcp relay
DHCP Relay Global Status: Enable
Interface     Status       Target Address
-------------------------------------------
 IP0         Disable      --
 IP1         Enable       10.1.2.1
 IP2         Disable      --
 IP3         Disable      --
…
```

Check the DHCP server.

Use the following command to show configurations of DHCP Server.

```
Qtech#show ip dhcp server
Global DHCP Server:  Enable
Global Minimum Lease: 30  minutes
Global Default Lease: 30  minutes
Global Maximum Lease: 10080minutes

Interface     Status       Pools bind
-------------------------------------------
 IP0         Enable       Qtech1
 IP1         Disable      --
 IP2         Disable      --
…
```

Use the following command to show the address pool of the DHCP server.

```
Qtech#show ip dhcp server pool Qtech1
Pool Name:          Qtech1
Associated Interface: IP0
Address Range:       10.1.1.5~10.1.1.10
Address Mask:        255.255.255.0
Gateway:            10.1.1.1
DNS Server:          10.1.1.4
Secondary DNS:       0.0.0.0
Tftp Server:         0.0.0.0
Bootfile:           --
Default Lease:       0    minutes
Minimum Lease:       0    minutes
Maximum Lease:       0    minutes
```

Use the following command to show configurations of the DHCP Relay device trusted by the DHCP server.

```
Qtech#show ip dhcp server relay-ip
Index    IP address        Mask
------------------------------------------
1       10.1.1.1          255.255.255.0
```

Check the DHCP client.

Use the following command to check whether the DHCP client has obtained the IP address.

```
Qtech#show ip dhcp client
  Hostname:                Qtech
  Class-ID:                Qtech-ROS
  Client-ID:               Qtech-001fce000010-IF0
  Assigned IP Addr:        10.1.1.5
  Subnet mask:             255.255.255.0
  Default Gateway:          10.1.1.1
  Client lease Starts:      Jan-01-2010 08:26:36
  Client lease Ends:        Jan-01-2010 08:56:36
  Client lease duration:    1800(sec)
  DHCP Server:              10.1.2.1
  Tftp server name:         --
  Tftp server IP Addr:      --
  Startup_config filename:   --
  NTP server IP Addr:       --
  Root path:               --
```

4.4 DHCP Snooping

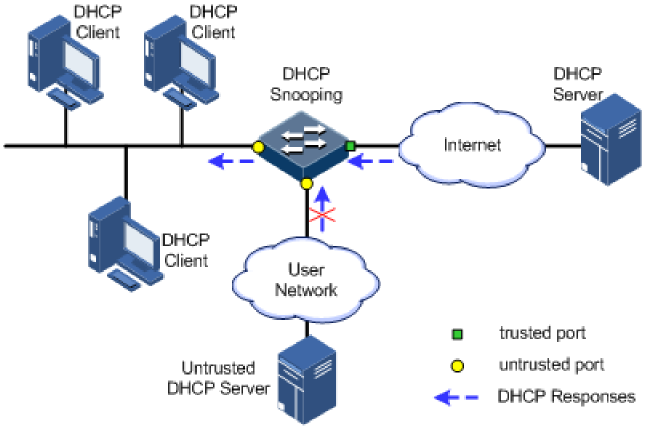
4.4.1 Introduction

DHCP Snooping is a security feature of DHCP with the following functions:

- Guarantee the DHCP client to obtain the IP address from a legal DHCP server.

If a forged DHCP server exists on the network, the DHCP client may obtain incorrect IP address and network configuration parameters, and thus cannot communicate normally. As shown in Figure 4-7, to make the DHCP client get the IP address from a legal DHCP server, the DHCP Snooping security system allows to set an interface as the trusted interface or untrusted interface: the trusted interface can forward DHCP packets normally; the untrusted interface discards the reply packets from the DHCP server.

Figure 4-7 DHCP Snooping networking



- Record corresponding relationship between IP address and MAC address of the DHCP client.

Through DHCP Snooping, the DHCP server records DHCP Snooping entries by listening requests and reply packets received on the trusted interface, including the MAC address of clients, obtained IP address, interface number connected to the DHCP client, and VLAN for the interface. Based on the information, the following functions can be realized:

  - ARP inspection: judge legality of a user that sends ARP packets and avoid ARP attack from illegal users.
  - IP Source Guard: filter packets forwarded by the interface by dynamically obtain DHCP Snooping entries to prevent illegal packets from passing the interface.

The Option field in DHCP packet records position information about DHCP clients. The administrator can use this option to locate the DHCP client and implement security control and accounting.

If the QSW-8200 series switch is configured with DHCP Snooping to support DHCP Option:

- When the QSW-8200 series switch receives a DHCP request packet, it processes the packet according to the processing policy configured by the user, padding mode, and whether the Option field is included or not, and then forwards the processed packet to the DHCP server.
- When the QSW-8200 series switch receives a DHCP reply packet, if the packet contains the Option field, delete the field and forward the packet to the DHCP client; if the packet does not contain the Option field, forward the packet directly.

4.4.2 Preparing for configurations

Scenario

DHCP Snooping is a security feature of DHCP, used to guarantee DHCP clients to obtain IP addresses from the legal DHCP server and record mapping between IP addresses and MAC addresses of DHCP clients.

The Option field in DHCP packet records position information about DHCP clients. The administrator can use this option to locate the DHCP client and implement security control and accounting. The device configured with DHCP Snooping and DHCP Option can process packets accordingly based on whether packets contain the Option field.

Prerequisite

DHCP Server/Client is mutually exclusive to DHCP Snooping/Replay. Namely, you cannot configure them concurrently on a device. DHCP Relay and DHCP Snooping can be enabled concurrently.

4.4.3 Default configurations of DHCP Snooping

Default configurations of DHCP Snooping are as below.

Function	Default value
Global DHCP Snooping status	Disable
Interface DHCP Snooping status	Enable
Interface trusted/untrusted status	Untrusted
DHCP Snooping supporting Option 82	Disable
DHCP Snooping supporting Option 61	Disable
DHCP Snooping supporting customized Options	Disable
Auto-saving the DHCP Snooping binding table	Disable
Interval for automatically saving the DHCP Snooping binding table	300s

4.4.4 Configuring DHCP Snooping

Generally, ensure that the QSW-8200 series switch interface connected to the DHCP server is in trust status while its interface connected to the user is in untrusted status.

Enabled with DHCP Snooping, if the QSW-8200 series switch is not configured with DHCP Snooping supporting DHCP Option, it will do nothing to Option fields for packets. For packets without Option fields, the QSW-8200 series switch still does not do insertion operation.

By default, DHCP Snooping on all interfaces is enabled. However, only after global DHCP Snooping is enabled can you enable DHCP Snooping on an interface.

Configuring DHCP Snooping over IPv4

Configure DHCP Snooping over IPv4 on the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**ip dhcp snooping**	Enable global DHCP Snooping over IPv4.
3	Qtech(config)#**ip dhcp snooping port-list** *port-list*	(Optional) enable interface DHCP Snooping over IPv4.
4	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
5	Qtech(config-port)#**ip dhcp snooping trust**	Configure the trusted interface over IPv4.
6	Qtech(config-port)#**ipv4 dhcp option** *number*	(Optional) configure DHCP Snooping to support DHCP Option defined by IPv4.
7	Qtech(config-port)#**exit** Qtech(config)#**ip dhcp snooping option client-id**	(Optional) configure DHCP Snooping to support the Option 61 feature.
8	Qtech(config)#**ip dhcp snooping information option**	(Optional) configure DHCP Snooping to support the Option 82 feature.

Configuring DHCP Snooping over IPv6

Configure DHCP Snooping over IPv6 for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**ipv6 dhcp snooping**	Enable global DHCP Snooping over IPv6.
3	Qtech(config)#**ipv6 dhcp snooping port-list** *port-list*	(Optional) enable interface DHCP Snooping over IPv6.
4	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
5	Qtech(config-port)#**ipv6 dhcp snooping trust** Qtech(config-port)#**exit**	Configure the trusted interface over IPv6.
6	Qtech(config)#**ipv6 dhcp snooping option** *number*	(Optional) configure DHCP Snooping to support customized the DHCP Option feature over IPv6.
7	Qtech(config)#**ipv6 dhcp snooping option interface-id**	(Optional) configure DHCP Snooping to support the Option 18 feature.

4.4.5 Configuring auto-saving for binding table

The QSW-8200 series switch supports automatical saving of the DHCP Snooping binding table. After this function is enabled, it backs up the learnt binding table periodically to the Flash. After it is restarted, it reads the saved binding table and rebuilds this binding table.

Note

- Only after DHCP Snooping is enabled can auto-saving of the DHCP Snooping binding table take effect.
- Before restarting the QSW-8200 series switch, save configurations so that the rebuilt binding table can take effect after restart.

Configure auto-saving for binding table for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**ip dhcp snooping autosave enable**	Enable auto-saving of DHCP Snooping binding table.
3	Qtech(config)#**ip dhcp snooping autosave write-delay** *time*	Configure the interval for automatically saving the DHCP Snooping binding table.

4.4.6 Checking configurations

Use the following commands to check configuration results.

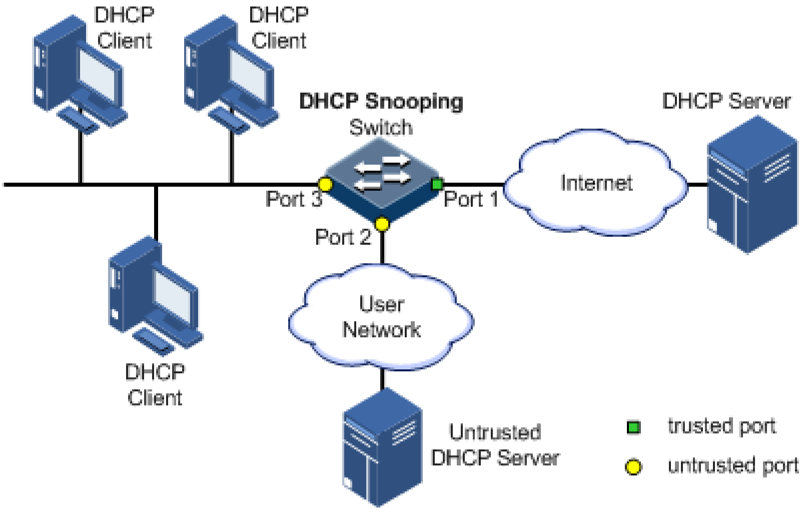
Step	Command	Description
1	Qtech#**show ip dhcp snooping**	Show configurations of DHCP Snooping over IPv4.
2	Qtech#**show ip dhcp snooping binding**	Show configurations of DHCP Snooping binding table over IPv4.

4.4.7 Example for configuring DHCP Snooping

Networking requirements

As shown in Figure 4-8, the Switch is used as a DHCP Snooping device. The network requires the DHCP client to obtain the IP address from a legal DHCP server and supports Option82 to facilitate client management; you can configure circuit ID sub-Option to port3 on port 3, and make the filling content of remote ID sub-option as the MAC address of the switch.

Figure 4-8 DHCP Snooping networking



Configuration steps

Step 1 Configure global DHCP Snooping.

```
Qtech#config
Qtech(config)#ip dhcp snooping
```

Step 2 Configure the trusted interface.

```
Qtech(config)#interface port 1
Qtech(config-port)#ip dhcp snooping trust
Qtech(config-port)#quit
```

Step 3 Configure DHCP Relay to support the Option 82 feature and configure the Option 82 field.

```
Qtech(config)#ip dhcp snooping information option
Qtech(config)#ip dhcp information option remote-id switch-mac
Qtech(config)#interface port 3
Qtech(config-port)#ip dhcp information option circuit-id port3
```

Checking results

Use the **show ip dhcp snooping** command to shows configurations of the DHCP server.

```
Qtech#show ip dhcp snooping
DHCP Snooping: Enabled
DHCP Option 82: Enabled
```

```
Port      Enabled Status     Trusted Status
---------------------------------------------------
P1       enabled          yes
P2       enabled          no
P3       enabled          no
…
```

Use the **show ip dhcp information option** command to show configurations of DHCP Option.

```
Qtech#show ip dhcp information option
DHCP Option Config Information
  Circuit-ID:   default
  Remote-ID Mode:  switch-mac
  P3   Circuit ID:  port3
ipv4Global
ipv4Port
P1:
P2:
P3:
…
```

4.5 DHCP Option

4.5.1 Introduction

DHCP transmits control information and network configuration parameters through option fields in packets to realize dynamical assignment of IP addresses to provide abundant network configurations for clients. DHCP has 255 types of options, and the final option is 255. Frequently used DHCP options are as below.

Options	Description
3	Router, to assign gateway for DHCP clients
6	DNS server, to assign DNS server address distributed by DHCP clients
18	DHCP client flag, used to assign interface information about DHCP client
51	IP address lease time
53	DHCP message type, used to identify the type of DHCP packets
61	DHCP client flag, to assign device information about DHCP clients
66	TFTP server name, to assign domain name for TFTP server distributed by DHCP clients
67	Bootfile name, used to assign the startup file name distributed by DHCP clients

Options	Description
82	DHCP client flag, user-defined, used to mark position of the DHCP client, including Circuit ID and remote ID
150	TFTP server address, used to specify the IP address of the TFTP server assigned for the DHCP client

Options 18, 61, and 82 in DHCP Option are relay agent information options in DHCP packets. When a request packet sent by the DHCP client arrives at the DHCP server with traversing a DHCP relay or DHCP Snooping, the DHCP relay or DHCP Snooping device adds Option fields into the request packet, and then forward the request packet to the DHCP server.

Options 18, 61, and 82 implement the recording of DHCP client information on the DHCP server. By using them with other software, the device can implement functions such as limiting on the assignment of IP addresses and accounting. For example, when you use them with IP Source Guard, the device can defend IP address+MAC address spoofing.

Option 82

Option 82, with its standard defined in RFC 3046, is a Relay Agent Information option in the DHCP packet. If a request packet sent from the DHCP client to the DHCP server traverses the DHCP Snooping device, the DHCP Snooping device adds Option 82 into the request packet.

Option 82 can contain multiples 255 sub-options. If Option82 is defined, at least one sub-option must be defined. The QSW-8200 series switch supports the following two sub-options:

- Sub-Option 1: a sub-option of Option 82, the circuit ID sub-option. A sub-option is configured on the DHCP Snooping device or DHCP Relay device. It contains the interface number of the request packet sent by the DHCP client, the VLAN that the interface belongs to, and attaching information about the DHCP Snooping device or DHCP Relay device which receives the request packet from the DHCP client during packet transmission.
- Sub-Option 2: a sub-option of Option 82, the remote ID sub-option. The sub-option contains the interface MAC address (DHCP relay), bridge MAC address (DHCP Snooping device), or customized character string contained in the request packet sent from the DHCP client to the DHCP Relay device or DHCP Snooping device during packet transmission.

The Sub-Option 1 and Sub-Option 2 are usually used together to identify the DHCP source. Options 82 implements the recording of DHCP client information on the DHCP server.

Options supported by device

The QSW-8200 series switch supports the following Options:

- Option 82 over IPv4
- Option 61 over IPv4
- Customized Option over IPv4
- Option 18 over IPv6
- Customized Option over IPv6

Note

- DHCP Option should be configured on the device that is enabled with DHCP Snooping or DHCP Relay.
- The device enabled with DHCP Relay supports Option 82 at present.

4.5.2 Preparing for configurations

Scenario

Options 18, 61, and 82 in DHCP Option are relay agent information options in DHCP packets. When a request packet sent by the DHCP client arrives at the DHCP server with traversing a DHCP relay or DHCP Snooping, the DHCP relay or DHCP Snooping device adds Option fields into the request packet.

DHCP Option 18 is used to record DHCP client information over IPv6. DHCP Options 61 and 82 fields are used to record DHCP client information over IPv4. By using them with other software, the device can implement functions such as limiting on the assignment of IP addresses and accounting.

Prerequisite

DHCP Option should be configured on the device that is enabled with DHCP Snooping or DHCP Relay. To make DHCP Option take effect, ensure that DHCP Snooping or DHCP Relay is enabled on the same device.

4.5.3 Default configurations of DHCP Option

Default configurations of DHCP Option are as below.

Function	Default value
attach-string in global configuration mode	N/A
remote-id in global configuration mode	switch-mac, interface MAC address of the DHCP Relay device or bridge MAC address of the DHCP Snooping device
circuit-id in interface configuration mode	N/A

4.5.4 Configuring DHCP Option 82 over IPv4

Configure DHCP Option 82 over IPv4 for the QSW-8200 series switch as below.

Option 82 should be configured on the device that is enabled with DHCP Snooping or DHCP Relay.

All the following steps are optional and in any sequence.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.

Step	Command	Description
2	Qtech(config)#**ip dhcp information option attach-string** *attach-string*	(Optional) configure attaching information about Option 82.
3	Qtech(config)#**ip dhcp information option circuit-id mac-format** *string*	(Optional) configure the format of the MAC address as a variable of Circuit ID of Option 82 in DHCP packets.
4	Qtech(config)#**interface** *interface-type interface-number* Qtech(config-port)#**ip dhcp information option circuit-id** *circuit-id*	(Optional) configure circuit ID sub-option information about Option 82 field on the interface.
5	Qtech(config-port)#**exit** Qtech(config)#**ip dhcp information option remote-id** { **client-mac** | **client-mac-string** | **hostname** | **switch-mac** | **switch-mac-string** | **string** *string* }	(Optional) configure remote ID sub-option information about Option 82.

4.5.5 Configuring DHCP Option 61 over IPv4

Configure DHCP Option 61 over IPv4 for the QSW-8200 series switch as below.

Option 61 should be configured on the device that is enabled with DHCP Snooping.

All the following steps are optional and in any sequence.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**ipv4 dhcp option client-id** { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* }	(Optional) configure information about Option 61.
3	Qtech(config)#**interface port** *port-id* Qtech(config-port)#**ipv4 dhcp option client-id** { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* }	(Optional) configure information about Option 61 on the interface.

4.5.6 Configuring customized DHCP Option over IPv4

Configure customized DHCP Option over IPv4 for the QSW-8200 series switch as below.

Customized DHCP Option should be configured on the device that is enabled with DHCP Snooping.

All the following steps are optional and in any sequence.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.

Step	Command	Description
2	Qtech(config)#**ipv4 dhcp option** *option-id* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* }	(Optional) create customized option information over IPv4.
3	Qtech(config)#**interface port** *port-id* Qtech(config-port)#**ipv4 dhcp option** *option-id* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* }	(Optional) create customized option information over IPv4 on the interface.

4.5.7 Configuring DHCP Option 18 field over IPv6

Configure DHCP Option 18 field over IPv6 for the QSW-8200 series switch as below.

Option 18 over IPv6 should be configured on the device that is enabled with DHCP Snooping.

All the following steps are optional and in any sequence.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**ipv6 dhcp option interface-id** { **ascii** *ascii-string* | **hex** *hex-string* | **ipv6-address** *ipv6-address* }	(Optional) configure information about Option 18.
3	Qtech(config)#**interface port** *port-id* Qtech(config-port)#**ipv6 dhcp option interface-id** { **ascii** *ascii-string* | **hex** *hex-string* | **ipv6-address** *ipv6-address* }	(Optional) configure information about Option 18 on the interface.

4.5.8 Configuring customized DHCP Option over IPv6

Configure customized DHCP Option over IPv6 for the QSW-8200 series switch as below.

Customized Option over IPv6 should be configured on the device that is enabled with DHCP Snooping.

All the following steps are optional and in any sequence.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config-port)#**exit** Qtech(config)#**ipv6 dhcp option** *number* { **ascii** *ascii-string* | **hex** *hex-string* | **ipv6-address** *ipv6-address* }	(Optional) create customized Option information over IPv6.
3	Qtech(config)#**interface port** *port-id* Qtech(config-port)#**ipv6 dhcp option** *number* { **ascii** *ascii-string* | **hex** *hex-string* | **ipv6-address** *ipv6-address* }	(Optional) create customized Option information over IPv6 on the interface.

4.5.9 Checking configurations

Use the following command to check configuration results.

No.	Command	Description
1	`Qtech#show ip dhcp information option`	Show configurations of DHCP Option fields.

5 QoS

This chapter describes basic principles and configurations of QoS, and provides related configuration examples, including the following sections:

- Introduction
- Configuring priority
- Configuring congestion management
- Configuring congestion avoidance
- Configuring traffic classification and traffic policy
- Configuring QoS enhancement
- Configuring rate limiting based on interface and VLAN
- Maintenance
- Configuring examples

5.1 Introduction

Users bring forward different service quality demands for network applications, then the network should distribute and schedule resources for different network applications according to user demands. Quality of Service (QoS) can ensure service in real time and integrity when network is overloaded or congested and guarantee that the whole network runs efficiently.

QoS is composed of a group of flow management technologies:

- Service model
- Priority trust
- Traffic classification
- Traffic policy
- Priority mapping
- Congestion management
- Congestion avoidance

5.1.1 Service model

QoS technical service models:

- Best-effort Service
- Differentiated Services (DiffServ)

Best-effort

Best-effort service is the most basic and simplest service model on the Internet (IPv4 standard) based on storing and forwarding mechanism. In Best-effort service model, the application can send a number of packets at any time without being allowed in advance and notifying the network. For Best-effort service, the network will send packets as possible as it can, but cannot guarantee the delay and reliability.

Best-effort is the default Internet service model now, applying to most network applications, such as FTP and E-mail, which is implemented by First In First Out (FIFO) queue.

DiffServ

DiffServ model is a multi-service model, which can satisfy different QoS requirements.

DiffServ model does not need to maintain state for each flow. It provides differentiated services according to the QoS classification of each packet. Many different methods can be used for classifying QoS packets, such as IP packet priority (IP precedence), the packet source address or destination address.

Generally, DiffServ is used to provide end-to-end QoS services for a number of important applications, which is implemented through the following techniques:

- Committed Access Rate (CAR): CAR refers to classifying the packets according to the pre-set packets matching rules, such as IP packets priority, the packet source address or destination address. The system continues to send the packets if the flow complies with the rules of token bucket; otherwise, it discards the packets or remarks IP precedence, DSCP, EXP, etc. CAR can not only control the flows, but also mark and remark the packets.
- Queue technology: the queue technologies of SP, WRR, DRR, SP+WRR, and SP+DRR cache and schedule the congestion packets to implement congestion management.

5.1.2 Priority trust

Priority trust refers to that the QSW-8200 series switch uses priority of packets for classification and performs QoS management.

The QSW-8200 series switch supports packet priority trust based on interface, including:

- Differentiated Services Code Point (DSCP) priority
- Class of Service (CoS) priority
- ToS priority

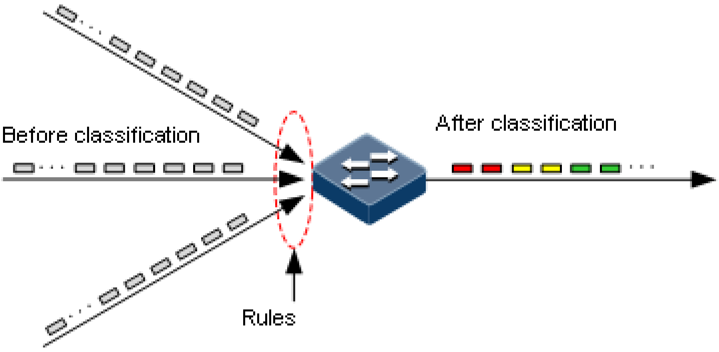
5.1.3 Traffic classification

Traffic classification refers to identifying certain packets according to specified rules and performing different QoS policies on packets matched with different rules. Traffic classification is the premise and basis for differentiated services.

The QSW-8200 series switch supports traffic classification based on ToS priority, DSCP priority, and CoS priority over IP packets, as well as the classification based on Access

Control List (ACL) rules and VLAN ID. The traffic classification procedure is shown in Figure 5-1.

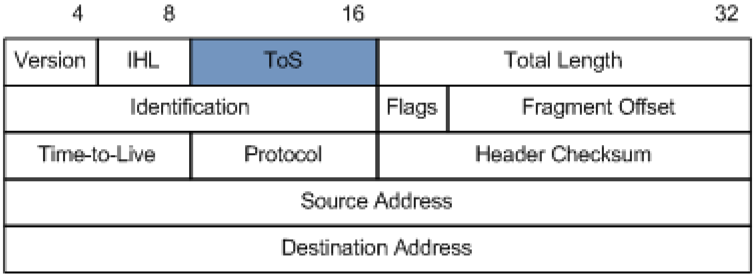
Figure 5-1 Traffic classification



IP priority and DSCP priority

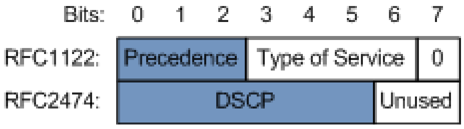
Figure 5-2 shows the structure of the IP packet head. The head contains an 8-bit ToS field. Defined by RFC 1122, IP priority (IP Precedence) uses the highest 3 bits (0–3) with value range of 0–7; RFC2474 defines ToS field again, and applies the first 6 bits (0–5) to DSCP priority with value range 0–63, the last 2 bits (bit-6 and bit-7) are reserved. Figure 5-3 shows the structures of ToS and DSCP priorities.

Figure 5-2 Structure of IP packet header



4	8	16		32
Version	IHL	ToS	Total Length	
Identification			Flags	Fragment Offset
Time-to-Live		Protocol	Header Checksum	
Source Address				
Destination Address				

Figure 5-3 Structures of ToS priority and DSCP priority

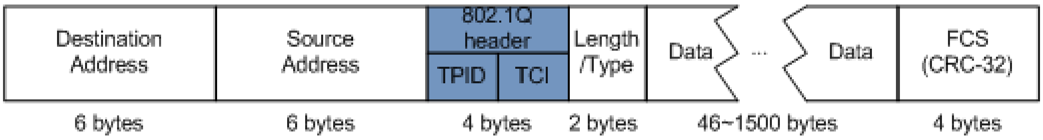


Bits:	0	1	2	3	4	5	6	7
RFC1122:	Precedence			Type of Service				0
RFC2474:	DSCP						Unused	

CoS priority

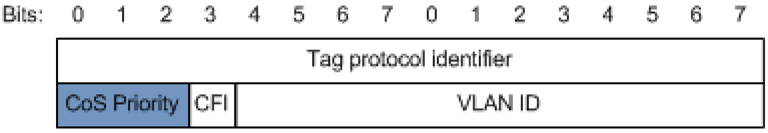
IEEE802.1Q-based VLAN packets are modifications of Ethernet packets. A 4-Byte 802.1Q header is added between the source MAC address and protocol type, as shown in Figure 5-4. The 802.1Q header consists of a 2-Byte Tag Protocol Identifier (TPID, valuing 0x8100) filed and a 2-Byte Tag Control Information (TCI) field.

Figure 5-4 Structure of VLAN packet



The first 3 bits of the TCI field represent the CoS priority, which ranges from 0 to 7, as shown in Figure 5-5. CoS priority is used to guarantee QoS on the Layer 2 network.

Figure 5-5 Structure of CoS priority



5.1.4 Traffic policy

After performing traffic classification on packets, you need to perform different operations on packets of different categories. A traffic policy is formed when traffic classifiers are bound to traffic behaviours.

Rate limiting based on traffic policy

Rate limiting refers to controlling network traffic, monitoring the rate of traffic entering the network, and discarding overflow part, so it controls ingress traffic in a reasonable range, thus protecting network resources and carrier interests.

The QSW-8200 series switch supports rate limiting based on traffic policy in the ingress direction on the interface.

The QSW-8200 series switch supports using token bucket for rate limiting, including single-token bucket and dual-token bucket.

Redirection

Re-direction refers to re-directing packets to a specified interface, instead of forwarding packets according to the mapping between the original destination address and interface, thus implementing policy routing.

The QSW-8200 series switch supports re-directing packets to the specified interface for forwarding in the ingress direction of an interface.

Re-marking

Re-mark refers to setting some priority fields in packet again and then classifying packets by user-defined standard. Besides, downstream nodes on the network can provide differentiated QoS service according to re-mark information.

The QSW-8200 series switch supports re-marking packets by the following priority fields:

- IP priority
- DSCP priority
- CoS priority

Traffic statistics

Traffic statistics is used to take statistics of data packets of a specified service flow, namely, the number of packets and Bytes matching traffic classification that pass the network or are discarded.

Traffic statistics is not a QoS control measure, but can be used in combination with other QoS actions to improve network supervision.

5.1.5 Priority mapping

Priority mapping refers to sending packets to different queues with different local priorities according to pre-configured mapping between external priority and local priority. Therefore, packets in different queues can be scheduled on the egress interface.

The QSW-8200 series switch supports performing priority mapping based on the DSCP priority of IP packets or the CoS priority of VLAN packets. The Traffic-Class field of IPv6 packets corresponds to the DSCP priority of IPv4 packets. The mapping from DSCP priority to local priority is applicable to IPv6 packets. Take the first 6 bits of the Traffic-Class field for use.

By default, the mapping between the QSW-8200 series switch local priority and DSCP, CoS priorities is listed in Table 5-1 and Table 5-2.

Table 5-1 Mapping between local priority and DSCP priority

Local	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
DSCP	0–7	8–15	16–23	24–31	32–39	40–47	48–55	56–63
CoS	0	1	2	3	4	5	6	7

Local priority refers to a kind of packet priority with internal meaning assigned by the QSW-8200 series switch and is the priority corresponding to queue in QoS queue scheduling.

Local priority ranges from 0 to 7. Each interface of the QSW-8200 series switch supports 8 queues. Local priority and interface queue is in one-to-one mapping. The packet can be sent to the assigned queue according to the mapping between local priority and queue, as shown in Table 5-2

Table 5-2 Mapping between local priority and queue

Local	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Queue	1	2	3	4	5	6	7	8

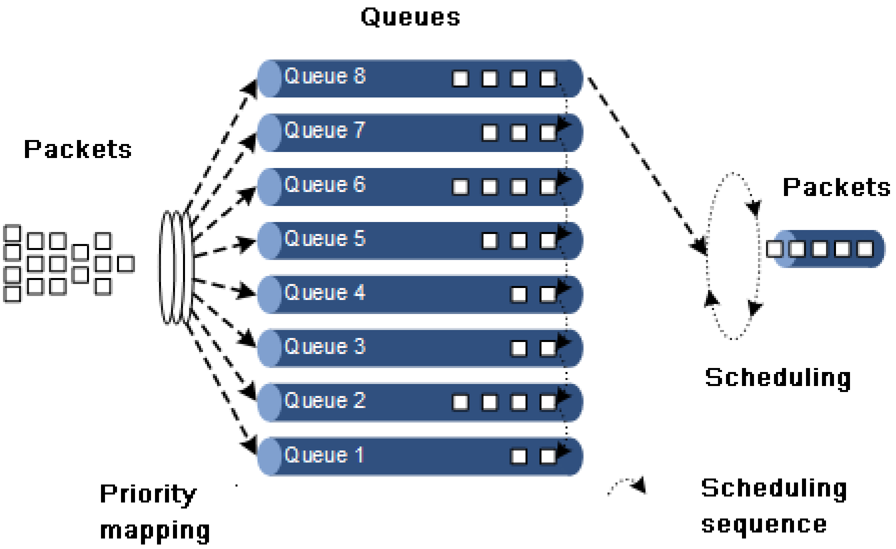
5.1.6 Queue scheduling

The QSW-8200 series switch needs to perform queue scheduling when delay-sensitive services need better QoS services than non-delay-sensitive services and when the network is congested once in a while.

Queue scheduling adopts different scheduling algorithms to send packets in a queue. Scheduling algorithms supported by the QSW-8200 series switch include Strict-Priority (SP), Weight Round Robin (WRR), Deficit Round Robin (DRR), SP+WRR, and SP+DRR. All scheduling algorithms are designed for addressing specified traffic problems. And they have different effects on bandwidth distribution, delay, and jitter.

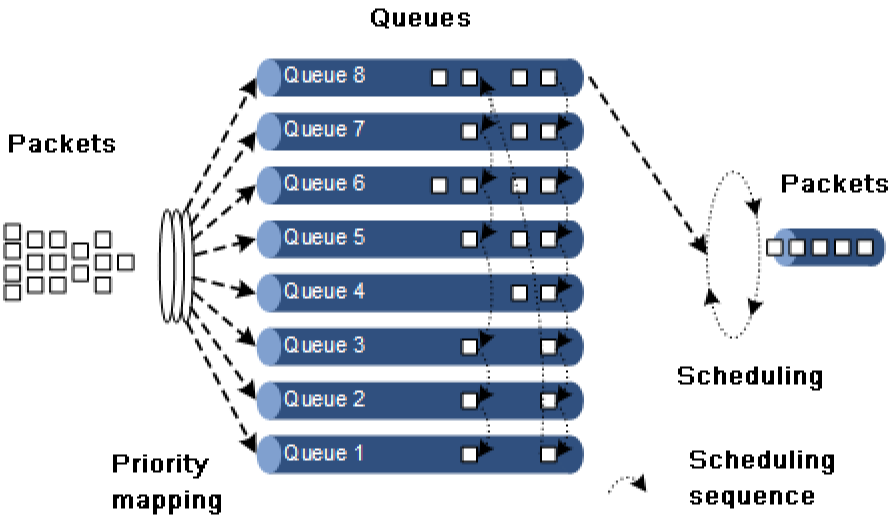
- SP: the QSW-8200-28F strictly schedules packets in a descending order of priority. Packets with lower priority cannot be scheduled until packets with higher priority are scheduled, as shown in Figure 5-6.

Figure 5-6 SP scheduling



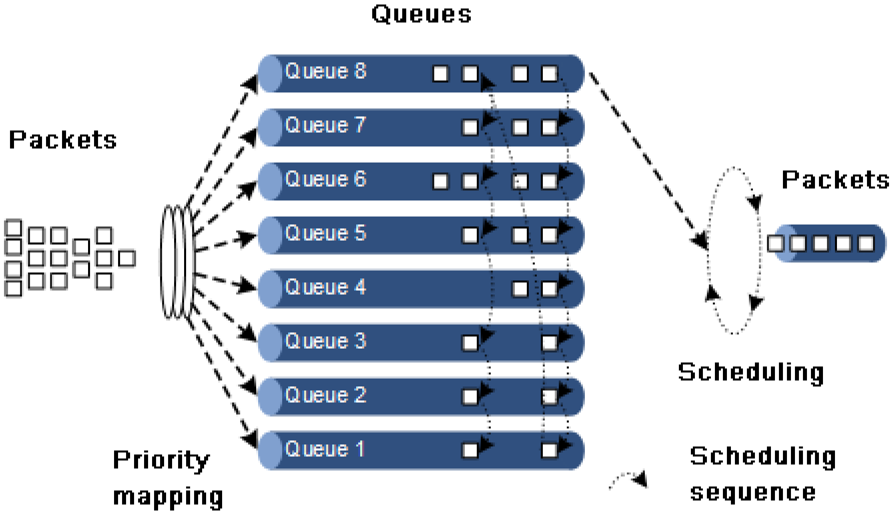
- WRR: on the basis of scheduling packets in a polling manner according to the priority, the QSW-8200-28F schedules packets according to the weight (based on Bytes) of the queue, as shown in Figure 5-7.

Figure 5-7 WRR scheduling



- DRR: similar with WRR, on the basis of scheduling packets in a polling manner according to the scheduling sequence, the QSW-8200-28F schedules packets according to the weight of the queue (based on packet), as shown in DRR scheduling

Figure 5-8 DRR scheduling



- SP+WRR: a scheduling mode combining the SP scheduling and WRR scheduling. In this mode, queues on an interface are divided into 2 groups. You can specify the queues where SP scheduling/WRR scheduling is performed.
- SP+DRR: a scheduling mode combining the SP scheduling and DRR scheduling. In this mode, queues on an interface are divided into 2 groups. You can specify the queues where SP scheduling/DRR scheduling is performed.

5.1.7 Congestion avoidance

By monitoring utilization of network resources (queues/memory buffer), congestion avoidance can discard packets actively when congestion occurs or when network traffic increases. It is a traffic control mechanism that is used to resolve network overload by adjusting network traffic.

The traditional packet loss policy uses the Tail-Drop mode to process all packets equally without differentiating class of services. When congestion occurs, packets at the end of a queue are discarded until congestion is resolved.

This Tail-Drop policy may cause TCP global synchronization, making network traffic change between heavy and low and affecting link utilization.

RED

The Random Early Detection (RED) technology discards packets randomly and makes multiple TCP connection not reduce transport speed simultaneously to avoid TCP global synchronization.

The RED algorithm set a minimum threshold and maximum threshold for length of each queue. In addition:

- Packets are not discarded when the queue length is smaller than the minimum threshold.
- All received packets are discarded when the queue length is greater than the maximum threshold.
- Packets to be received are discarded randomly when the queue length is between the minimum and maximum thresholds. The greater the queue size is, the higher the packet drop probability is.

WRED

The Weighted Random Early Detection (WRED) technology also discards packets randomly to avoid TCP global synchronization. However, the random drop parameter generated by WRED technology is based on the priority. WRED differentiates drop policies through the color of packets. This helps ensure that high-priority packets have a smaller packet drop probability.

The QSW-8200 series switch supports WRED congestion avoidance but only supports the queue scheduling in the egress interface.

5.1.8 Rate limiting based on interface and VLAN

The QSW-8200 series switch supports rate limiting both based on traffic policy and based on interface or VLAN ID. Similar to rate limiting based on traffic policy, the QSW-8200 series switch discards the exceeding traffic.

5.1.9 QoS enhancement

QoS enhancement is a sub-function of QoS, and it is more flexible than basic QoS. It is widely used on the Switch.

QoS enhancement has the following functions:

- The ingress interface
  - Bandwidth guarantee: bandwidth service based on interface or flow is implemented. QoS enhancement supports hierarchical bandwidth guarantee and divides bandwidth more detailed for different service flows.
  - Awaring: this function decides whether to conduct color awaring of packets when a flow enters the bandwidth-guaranteed interface.
- The egress interface
  - Bandwidth guarantee: bandwidth service based on interface or flow is implemented. QoS enhancement does not support hierarchical bandwidth guarantee.
  - Marking: this function decides whether to mark a packet with color when a flow leaves the bandwidth-guaranteed interface.

Bandwidth guarantee

The bandwidth guarantee function guarantees that the traffic entering the network is within the defined range, and it discards or schedules packets. Bandwidth guarantee can meet users' requirements on service bandwidth, and also protect network resources and carriers' benefits.

By configuring the bandwidth guarantee profile and applying it to an interface, you can mark different flows green, yellow, and red. The QSW-8200 series switch takes different actions over flows of different colors: forward green flows, schedule yellow flows, and discard red flows.

Hierarchical bandwidth guarantee

Hierarchical bandwidth guarantee is a more flexible bandwidth guarantee. You can configure guaranteed bandwidth for each flow independently and even configure guaranteed bandwidth for sum of multiple flows through hierarchical bandwidth guarantee.

Color awaring and marking

If enabled with color awaring, the QSW-8200 series switch is in Color-aware status, in which it can identify whether the ingress flow is marked with color. If disabled with color awaring, the QSW-8200 series switch is in Color-blind status, in which it can neglect whether the ingress flow is marked with color, but identify the flow color again.

The function of color marking judges the color of a flow according to Committed Information Rate (CIR), Committed Burst Size (CBS), Excess Information Rate (EIR), and Excess Burst Size (EBS) configured in the bandwidth guarantee profile, and modifies the flag bit to mark it with color according to the packet format defined in 802.1ad.

5.2 Configuring priority

5.2.1 Preparing for configurations

Scenario

You can choose priority for trusted packets from upstream devices. Untrusted priority packets are processed by traffic classification and traffic policy. After configuring priority trust mode, the QSW-8200 series switch processes packets according to their priorities and provides related service.

To specify local priority for packets is the prerequisite for queue scheduling. For packets from the upstream device, you can map external priorities carried by packets to different local priorities, and configure local priorities for packets based on interface. Then the QSW-8200 series switch will take queue scheduling according to local priority of packets. Generally, IP packets need to be configured with mapping between IP priority/DSCP priority and local priority; while VLAN packets need to be configured with mapping between CoS priority and local priority.

Prerequisite

N/A

5.2.2 Default configurations of basic QoS

Default configurations of basic QoS are as below.

Function	Default value
Global QoS status	Enable
Interface trust priority type	Trust CoS priority
CoS to local priority and color mapping	See Table 5-3.
DSCP to local priority and color mapping	See Table 5-4.
ToS to local priority and color mapping	See Table 5-5.
Interface priority	0

Table 5-3 Default mapping from CoS to local priority and color

CoS	0	1	2	3	4	5	6	7
Local	0 (green)	1 (green)	2 (green)	3 (green)	4 (green)	5 (green)	6 (green)	7 (green)

Table 5-4 Default mapping from DSCP to local priority and color

DSCP	0–7	8–15	16–23	24–31	32–39	40–47	48–55	56–63
Local	0 (green)	1 (green)	2 (green)	3 (green)	4 (green)	5 (green)	6 (green)	7 (green)

Table 5-5 Default mapping from ToS to local priority and color

ToS	0	1	2	3	4	5	6	7
Local	0 (green)	1 (green)	2 (green)	3 (green)	4 (green)	5 (green)	6 (green)	7 (green)

5.2.3 Enabling global QoS

Enable global QoS for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`mls qos enable`**	Enable global QoS. By default, the QSW-8200 series switch is enabled with global QoS. Use the **mls qos disable** command to disable this function.

5.2.4 Configuring interface trust priority type

Configure interface trust priority type for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Qtech(config-port)#`**`mls qos trust { cos [ inner ] | dscp | port-priority | tos }`**	Configure interface trust priority type. CoS priority exists in 802.1Q packet header. When it is used, the interface type must be Trunk Tunnel.

Step	Command	Description
4	Qtech(config-port)#**mls qos port-priority** *portpri-value*	Configure interface priority.

5.2.5 Configuring mapping from CoS to local priority and color

Configure mapping from CoS to local priority and color for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**mls qos mapping cos-to-local-priority** *profile-id*	Create a profile of mapping from CoS to local priority and color, and enter cos-to-pri configuration mode.
3	Qtech(cos-to-pri)#**cos** *cos-value* **to local-priority** *localpri-value* [**color** { **green** | **red** | **yellow** }]	(Optional) modify the profile of mapping from CoS to local priority and color.
4	Qtech(cos-to-pri)#**cos** *cos-value* **drop**	Configure the global profile of mapping from CoS to local priority and color.
5	Qtech(cos-to-pri)#**exit** Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
6	Qtech(config-port)#**mls qos cos-to-local-priority** *profile-id*	Apply the profile of mapping from CoS to local priority and color on the interface.

5.2.6 Configuring mapping from DSCP to local priority and color

Configure mapping from DSCP to local priority and color for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**mls qos mapping dscp-to-local-priority** *profile-id*	Create a profile of mapping from DSCP to local priority and color, and enter dscp-to-pri configuration mode.
3	Qtech(dscp-to-pri)#**dscp** *dscp-value* **to local-priority** *localpri-value* [**color** { **green** | **red** | **yellow** }]	(Optional) modify the profile of mapping from DSCP to local priority and color.
4	Qtech(dscp-to-pri)#**exit** Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.

Step	Command	Description
5	Qtech(config-port)#**mls qos dscp-to-local-priority** *profile-id*	Apply the profile of mapping from DSCP to local priority and color on the interface.

5.2.7 Configuring mapping from ToS to local priority and color

Configure mapping from ToS to local priority and color for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**mls qos mapping tos-to-local-priority** *profile-id*	Create a profile of mapping from ToS to local priority and color, and enter dscp-to-pri configuration mode.
3	Qtech(dscp-to-pri)#**tos** *tos-value* **to local-priority** *localpri-value* [**color** { **green** | **red** | **yellow** }]	(Optional) modify the profile of mapping from ToS to local priority and color.
4	Qtech(dscp-to-pri)#**exit** Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
5	Qtech(config-port)#**mls qos tos-to-local-priority** *profile-id*	Apply the profile of mapping from ToS to local priority and color on the interface.

5.2.8 Configuring DSCP mutation

Configure DSCP mutation for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**mls qos mapping dscp-mutation** *profile-id*	Create a DSCP mutation mapping profile, and enter dscp mutation configuration mode.
3	Qtech(dscp-mutation)#**dscp** *dscp-value* **to new-dscp** *newdscp-value*	(Optional) modify the DSCP mutation profile.
4	Qtech(dscp-mutation)#**exit** Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
5	Qtech(config-port)#**mls qos dscp-mutation** *profile-id*	Apply the DSCP mutation profile on the interface.

5.2.9 Configuring CoS re-marking

Configure CoS re-marking for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#mls qos mapping cos-remark` *`profile-id`*	Create a CoS re-marking profile, and enter cos-remark configuration mode.
3	`Qtech(cos-remark)#local-priority` *`localpri-value`* `to cos` *`newcos-value`*	Modify the CoS re-marking profile.

4	`Qtech(dscp-mutation)#exit`
	`Qtech(config)#interface port` *`port-id`*
		Enter physical layer interface configuration mode.

5	`Qtech(config-port)#mls qos cos-remark` *`profile-id`*	Apply the DSCP remark profile on the interface.

5.2.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Qtech#show mls qos`	Show global QoS status and WRED profile status.
2	`Qtech#show mls qos port-list` *`port-list`*	Show QoS priority, trust mode and scheduling mode on the interface.
3	`Qtech#show mls qos mapping cos-to-local-priority [` *`profile-id`* `]`	Show configurations of the profile mapping from CoS to local priority and color.
4	`Qtech#show mls qos mapping dscp-to-local-priority [` *`profile-id`* `]`	Show configurations of the profile mapping from DSCP to local priority and color.
5	`Qtech#show mls qos cos-to-local-priority port-list` *`port-list`*	Show application of the profile for mapping from CoS to local priority and color mapping profile on the interface.
6	`Qtech#show mls qos dscp-to-local-priority port-list` *`port-list`*	Show application of the profile for mapping from DSCP to local priority and color mapping profile on the interface.
7	`Qtech#show mls qos mapping dscp-mutation [` *`profile-id`* `]`	Show DSCP mutation profile mapping.
8	`Qtech#show mls qos dscp-mutation port-list` *`port-list`*	Show application of the profile for mapping from the ToS to local priority and color mapping profile on the interface.

No.	Command	Description
9	`Qtech#show mls qos mapping cos-remark [ profile-id ]`	Show application of the DSCP mutation profile on the interface.
10	`Qtech#show mls qos cos-remark port-list port-list`	Show information about the CoS remark profile.
11	`Qtech#show mls qos mapping tos-to-local-priority [ profile-id ]`	Show configurations of the profile mapping from ToS to local priority and color.
12	`Qtech# show mls qos tos-to-local-priority port port-list`	Show application of the profile for mapping from ToS to local priority and color mapping profile on the interface.

5.3 Configuring congestion management

5.3.1 Preparing for configurations

Scenario

When the network is congested, you can configure queue scheduling if you wish to:

- Balance delay and delay jitter of various packets, preferentially process packets of key services (like video and voice).
- Fairly process packets of secondary services (like E-mail) with identical priority.
- Process packets of different priorities according to respective weight values.

The scheduling algorithm to be chosen depends on the current service condition and customer requirements.

Prerequisite

Enable global QoS.

5.3.2 Default configurations of congestion management

Default configurations of congestion management are as below.

Function	Default value
Queue schedule mode	SP
Queue weight	• WRR weight for scheduling 8 queues is 1. • DRR weight for scheduling 8 queues is 1.

5.3.3 Configuring SP queue scheduling

Configure SP queue scheduling on the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**mls qos queue scheduler sp**	Configure queue scheduling mode as SP on the interface.

5.3.4 Configuring WRR or SP+WRR queue scheduling

Configure WRR or SP+WRR for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**mls qos queue scheduler wrr**	Configure queue scheduling mode as WRR on the interface.
4	Qtech(config-port)#**mls qos queue wrr** *weigh1 weight2 weight3…weight8*	Configure weight for various queues. Perform SP scheduling when the priority of some queue is 0.

5.3.5 Configuring DRR or SP+DRR queue scheduling

Configure DRR or SP+DRR on the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**mls qos queue scheduler drr**	Configure queue scheduling mode as DRR on the interface.
4	Qtech(config-port)#**mls qos queue drr** *weigh1 weight2 weight3…weight8*	Configure packet queue scheduling mode as DRR, and configure weight for various queues. Perform SP scheduling when priority of some queue is 0.

5.3.6 Configuring queue bandwidth guarantee

Configure queue bandwidth guarantee on the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Qtech(config-port)`**`mls qos queue`** *`queue-id`* **`shaping`** *`minband maxband`*	(Optional) configure bandwidth guarantee based on interface queue, without concerning burst size.
4	`Qtech(config-port)#` **`mls qos queue`** *`queue-id`* **`shaping cir`** *`minband`* **`cbs`** *`minburst`* **`pir`** *`maxband`* `[` **`pbs`** *`maxburst`* `]`	(Optional) configure bandwidth guarantee based on interface queue, and set the burst size.

5.3.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Qtech#`**`show mls qos port-list`** *`port-list`*	Show interface QoS priority, trust mode and schedule mode.
2	`Qtech#`**`show mls qos queue port-list`** *`port-list`*	Show queue weights on the interface.
3	`Qtech#`**`show mls qos queue shaping port-list`** *`port-list`*	Show bandwidth guarantee based on interface queue.

5.4 Configuring congestion avoidance

5.4.1 Preparing for configurations

Scenario

To avoid network congestion and solve the problem of TCP global synchronization, you can configure congestion avoidance to adjust network flow and relieve network overload.

The QSW-8200 series switch conducts congestion avoidance based on WRED.

Prerequisite

Enable global QoS.

5.4.2 Default configurations of congestion avoidance

Default configurations of congestion avoidance are as below.

Function	Default value
Global WRED status	Enable

5.4.3 Configuring WRED

Configure WRED for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`mls qos wred enable`**	Enable global WRED.
3	`Qtech(config)#`**`mls qos wred profile`** *`profile-id`*	Create a WRED profile, and enter WRED configuration mode.
4	`Qtech(wred)#`**`wred`** `[` **`color`** `{` **`green`** `|` **`red`** `|` **`yellow`** `} ]` **`start-drop-threshold`** *`start-drop`* **`end-drop-threshold`** *`end-drop`* **`max-drop-probability`** *`max-drop`*	Modify the WRED profile.

5	`Qtech(wred)#`**`exit`**
	`Qtech(config)#`**`interface port 2`**
		Enter physical layer interface configuration mode.

6	`Qtech(config-port)#`**`mls qos queue`** *`queue-id`* **`wredprofile`** *`wredprofile-num`*	Apply the WRED to the interface.

5.4.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Qtech#`**`show mls qos wred profile`** `[` *`profile-id`* `]`	Show information about the WRED profile.
2	`Qtech#`**`show mls qos queue wredprofile port-list`** *`port-list`*	Show application of the WRED profile on the interface.

5.5 Configuring traffic classification and traffic policy

5.5.1 Preparing for configurations

Scenario

Traffic classification is the basis of QoS. You can classify packets from the upstream device according to the priorities and ACL rules. After classification, the QSW-8200 series switch can perform corresponding operations on packets in different categories and provide corresponding services.

A traffic classification rule will not take effect until it is bound to a traffic policy. Apply traffic policy according to current network loading conditions and period. Usually, the QSW-8200 series switch limits the rate of transmitting packets according to configured rate when packets enter the network, and re-marks priority according to service feature of packets.

Prerequisite

Enable global QoS.

5.5.2 Default configurations of traffic classification and traffic policy

Default configurations of traffic classification and traffic policy are as below.

Function	Default value
Traffic policy status	Disable
Traffic policy statistics status	Disable

5.5.3 Enabling traffic policy

Enable traffic policy for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`policy enable`**	Enable global traffic policy. By default, this function is disabled. Use the **policy disable** to disable this function.

5.5.4 Creating traffic classification

Create traffic classification for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.

Step	Command	Description
2	Qtech(config)#**class-map** *class-map-name* [**match-all** | **match-any**]	Create traffic classification and enter traffic classification cmap configuration mode.
3	Qtech(config-cmap)#**description** *string*	(Optional) describe traffic classification.

5.5.5 Configuring traffic classification rules

Configure traffic classification rules for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**class-map** *class-map-name* [**match-all** | **match-any**]	Create traffic classification, and enter traffic classification cmap configuration mode.
3	Qtech(config-cmap)#**match** { **access-list-map** | **ip-access-list** | **ipv6-access-list** | **mac-access-list** } *acl-number*	(Optional) configure traffic classification over ACL rule. The ACL rule must be defined firstly and the type must be **permit**.
4	Qtech(config-cmap)#**match class-map** *class-map-name*	(Optional) configure traffic classification over traffic classification rule. The pursuant traffic classification must be created and the matched type must be identical with the traffic classification type.
5	Qtech(config-cmap)#**match cos** *cos-value*	(Optional) configure traffic classification over CoS priority of packets.
6	Qtech(config-cmap)#**match inner-vlan** *inner-vlan-value* **outer-vlan** *outer-vlan-value*	(Optional) configure traffic classification over inner VLAN of packets.
7	Qtech(config-cmap)#**match** { **ip dscp** *dscp-value* | **ip precedence** *ip-precedence-value* }	(Optional) configure traffic classification over DSCP priority or IP priority rule.
8	Qtech(config-cmap)#**match ipv6 flow-label** *label-list*	(Optional) configure traffic classification over flow label field of IPv6 packets.
9	Qtech(config-cmap)#**match** { **tunnel** | **vc** } { **exp** *exp-value* | **label** *label* }	(Optional) configure traffic classification over tunnel or virtual circuit label.
10	Qtech(config-cmap)#**match vlan** *vlan-id* [**double-tagging inner**]	(Optional) configure traffic classification over VLAN ID rule of VLAN packets.

Note

- When the matched type of a traffic classification is **match-all**, the matched information may have conflict and the configuration may fail.
- Traffic classification rules must be created for traffic classification; namely, the **match** parameter must be configured.
- For traffic classification quoted by traffic policy, do not modify traffic classification rule; namely, do not modify the **match** parameter of traffic classification.

5.5.6 Creating rate limiting rule and shaping rule

When you need to conduct rate limiting to packets based on traffic policy, create token buckets and set rate limiting and shaping rule to token bucket as well as quote this rule to traffic classification bound to traffic policy.

Create rate limiting rule for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**policer** *policer-name* [**aggregate** | **class** | **hierarchy** | **single**]	Create token buckets and enter traffic-policer configuration mode.
3	Qtech(traffic-policer)#**cir** *cir* **cbs** *cbs*	(Optional) configure Flow mode token bucket parameters. Note The flow mode token bucket is single token bucket, and only supports being configured with red and green packet operation.
4	Qtech(traffic-policer)#**cir** *cir* **cbs** *cbs* **ebs** *ebs*	(Optional) configure RFC2697 mode token bucket parameters.
5	Qtech(traffic-policer)#**cir** *cir* **cbs** *cbs* **pir** *pir* **pbs** *pbs*	(Optional) configure RFC2698 mode token bucket parameters.
6	Qtech(traffic-policer)#**cir** *cir* **cbs** *cbs* **eir** *eir* **ebs** *ebs* [**coupling**]	(Optional) configure RFC4115 mode or MEF token bucket parameters.
7	Qtech(traffic-policer)#**color-mode** { **aware** | **blind** }	(Optional) configure token bucket color mode.
8	Qtech(traffic-policer)#**copy-to-cpu** { **green** [**red** | **yellow** [**red**]] | **red** | **yellow** [**red**] }	(Optional) copy different color packets to CPU.
9	Qtech(traffic-policer)#**drop-color** { **red** [**yellow**] | **yellow** }	(Optional) configure token bucket to discard some packets in certain color.

Step	Command	Description
10	Qtech(traffic-policer)#**recolor** { **green-recolor** { **red** | **yellow** } | **red-recolor** { **green** | **yellow** } | **yellow-recolor** { **green** | **red** } }	(Optional) recolor packets.
11	Qtech(traffic-policer)#**set-cos** { **green** *green-value* [**red** *red-value* | **yellow** *yellow-value* [**red** *red-value*]] | **red** *red-value* | **yellow** *yellow-value* [**red** *red-value*] }	(Optional) configure the mapping from packet color to CoS value.
12	Qtech(traffic-policer)#**set-dscp** { **green** *green-value* [**red** *red-value* | **yellow** *yellow-value* [**red** *red-value*]] | **red** *red-value* | **yellow** *yellow-value* [**red** *red-value*] }	(Optional) configure the mapping from packet color to DSCP value.
13	Qtech(traffic-policer)#**set-pri** { **green** *green-value* [**red** *red-value* | **yellow** *yellow-value* [**red** *red-value*]] | **red** *red-value* | **yellow** *yellow-value* [**red** *red-value*] }	(Optional) configure the mapping from packet color to local priority.

5.5.7 Creating traffic policy

Create traffic policy for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**policy-map** *policy-map-name*	Create traffic policy, and enter traffic policy pmap configuration mode.
3	Qtech(config-pmap)#**description** *string*	(Optional) describe traffic policy.

5.5.8 Defining traffic policy mapping

Note

You can define one or more defined traffic classifications in one traffic policy.

Define traffic policy mapping for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**policy-map** *policy-map-name*	Create traffic policy and enter traffic policy pmap configuration mode.

Step	Command	Description
3	Qtech(config-pmap)#**class-map** *class-map-name*	Bind traffic classification into traffic policy; only apply traffic policy to packets matching with traffic classification. Note At least one type of rules must be created for traffic classification to be bound with traffic policy; otherwise, the binding will fail.

5.5.9 Defining traffic policy operation

Note

Define different operations to different flows in policy.

Define traffic policy operation for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**policy-map** *policy-map-name*	Create traffic policy, and enter traffic policy pmap configuration mode.
3	Qtech(config-pmap)#**class-map** *class-map-name*	Bind traffic classification with traffic policy; only apply traffic policy to packets matching with traffic classification. Note At least one type of rules must be created for traffic classification to be bound with traffic policy; otherwise, the binding will fail.
4	Qtech(config-pmap-c)#**police** *policer-name*	(Optional) apply token bucket on traffic policy and conduct rate limiting and shaping. Note Create the token bucket in advance, and configure rate limiting and shaping rules; otherwise, the operation will fail.
5	Qtech(config-pmap-c)#**hierarchy-police** *policer-name*	(Optional) bring in a hierarchy rate limiting rule in traffic policy. Note Hierarchy token bucket needs to be used with token buckets in other modes.

Step	Command	Description
6	Qtech(config-pmap-c)#**redirect-to port** *port-id*	(Optional) configure re-direct rule under traffic classification, forwarding classified packets from assigned interface.
7	Qtech(config-pmap-c)#**set** { **cos** *cos-value* | **inner-vlan** *inner-vlan-id* | **ip dscp** *ip-dscp-value* | **ip precedence** *ip-precedence-value* | **vlan** *vlan-id* }	(Optional) configure re-mark rule under traffic classification, modify packet CoS priority, inner VLAN, DSCP priority, IP priority, and VLAN ID.
8	Qtech(config-pmap-c)#**copy-to-mirror**	(Optional) configure flow mirroring to the monitor port.
9	Qtech(config-pmap-c)#**statistics enable**	(Optional) configure flow statistic rule under traffic classification, statistic packets for matched traffic classification.

5.5.10 Applying traffic policy to interfaces

Apply traffic policy to the interface for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**policy enable**	Enable traffic policy function.
3	Qtech(config)#**service-policy** *policy-name* { **egress** | **ingress** } **port-list** *port-list*	Apply the configured traffic policies in batches to the ingress or egress interface.
4	Qtech(config)#**service-policy** *policy-name* **ingress port-list** *port-list* **egress port-list** *port-list*	Apply the configured traffic policies in batches to the ingress and egress interface.

5.5.11 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show service-policy statistics** [**port** *port-id*]	Show traffic policy status and the applied policy statistics.
2	Qtech#**show class-map** [*class-map-name*]	Show traffic classification information.

No.	Command	Description
3	`Qtech#show policy-map [ policy-map-name ]`	Show traffic policy information.
4	`Qtech#show policy-map [ policy-map-name ] [ class class-map-name ]`	Show traffic classification information in traffic policy.
5	`Qtech#show mls qos policer [ policer-name ]`	Show assigned token bucket (rate limiting and shaping) information.
6	`Qtech#show mls qos policer-type [ aggregate-policer | class-policer | hierarchy-policer | single-policer ]`	Show assigned type token bucket (rate limiting and shaping) information.
7	`Qtech#show policy-map port [ port-id ]`	Show traffic policy application information on the interface.
8	`Qtech#show mls qos port-list port-id policers`	Show information about rate limiting rules on the interface.

5.6 Configuring QoS enhancement

5.6.1 Preparing for configurations

Scenario

QoS enhancement is used to guarantee service bandwidth for users and protect network resources and carriers' profits.

Prerequisite

N/A

5.6.2 Default configurations of QoS enhancement

Default configurations of QoS enhancement are as below.

Function	Default value
Color marking	Disable
Color awaring	Disable

5.6.3 Configuring bandwidth guarantee

Configure bandwidth guarantee for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**bandwidth-profile** *profile-id* **cir** *cir* **cbs** *cbs* [**color-aware**] Qtech(config)#**bandwidth-profile** *profile-id* **cir** *cir* **cbs** *cbs* **eir** *eir* **ebs** *ebs* [**color-aware** [**coupling**]]	Create a bandwidth guarantee profile.
3	Qtech(config)#**bandwidth** { **egress** | **ingress** } *interface-type interface-number profile-id*	Bind the bandwidth guarantee profile based on interface.
4	Qtech(config)#**bandwidth** { **egress** | **ingress** } *interface-type interface-number* **vlan** *vlan-id profile-id*	Bind the bandwidth guarantee profile based on interface+VLAN.
5	Qtech(config)#**bandwidth** { **egress** | **ingress** } *interface-type interface-number* **vlan** *vlan-id* **coslist** *coslist profile-id*	Bind the bandwidth guarantee profile based on interface+VLAN+CoS.

Note

If a bandwidth guarantee profile is used by other profiles or applied, it cannot be deleted.

5.6.4 Configuring hierarchical bandwidth guarantee

Creating hierarchical CoS bandwidth guarantee

Create hierarchical CoS bandwidth guarantee for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**bandwidth-profile** *bwp-index* **cir** *cir* **cbs** *cbs* [**eir** *eir* **ebs** *ebs*] [**color-aware**]	Create a bandwidth guarantee profile.
3	Qtech(config)#**hierarchy-cos bandwidth-profile** *hc-bwp-index*	Create a hierarchical CoS profile, and enter Hcos configuration mode.
4	Qtech(config-hcos)#**bandwidth coslist** *cos-list bwp-index* Qtech(config-hcos)#**exit**	Configure the hierarchical CoS profile.
5	Qtech(config)#**bandwidth ingress** *interface-type interface-number* **vlan** *vlan-id bwp-index* **hierarchy-cos** *hc-bwp-index*	Apply the hierarchical CoS profile on the egress interface+VLAN.

Creating hierarchical VLAN bandwidth guarantee

Create hierarchical VLAN bandwidth guarantee for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**bandwidth-profile** *bwp-index* **cir** *cir* **cbs** *cbs* [**eir** *eir* **ebs** *ebs*] [**color-aware**]	Create a bandwidth guarantee profile.
3	Qtech(config)#**hierarchy-vlan bandwidth-profile** *hv-bwp-index*	Create a hierarchical VLAN profile, and enter Hvlan configuration mode.
4	Qtech(config-hvlan)#**bandwidth vlanlist** *vlan-list bwp-index* Qtech(config-hvlan)#**exit**	Configure the hierarchical VLAN profile.
5	Qtech(config)#**bandwidth ingress** *interface-type interface-number bwp-index* **hierarchy-vlan** *hv-bwp-index*	Apply the hierarchical VLAN profile on the egress interface.

Note

If a hierarchical bandwidth guarantee profile is applied, it cannot be deleted or modified.

5.6.5 Configuring color awaring and marking

Configure color awaring and marking for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**bandwidth color-aware enable**	Enable color awaring of ingress packets on the bandwidth-guaranteed interface.
4	Qtech(config-port)#**bandwidth dei enable**	Enable color marking of egress packets on the bandwidth-guaranteed interface.

5.6.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Qtech#`**`show bandwidth-profile`** `[` *`bwp-index`* `]`	Show information about the bandwidth guarantee profile.
2	`Qtech#`**`show bandwidth`** *`interface-type interface-number`*	Show configurations of bandwidth guarantee and interface+hierarchical VLAN.
3	`Qtech#`**`show bandwidth`** *`interface-type interface-number`* **`vlan`** *`vlanid`*	Show configurations of interface+VLAN bandwidth guarantee and interface+VLAN+hierarchical CoS.
4	`Qtech#`**`show hierarchy-cos-bandwidth profile`** `[` *`hc-bwp-index`* `]`	Show information about the hierarchical CoS bandwidth guarantee profile.
5	`Qtech#`**`show hierarchy-vlan-bandwidth profile`** `[` *`hv-bwp-index`* `]`	Show information about the hierarchical VLAN bandwidth guarantee profile.
6	`Qtech#`**`show bandwidth-status port-list`** *`port-list`*	Show configurations of packet color awaring and mark on the bandwidth-guaranteed interface.

5.7 Configuring rate limiting based on interface and VLAN

5.7.1 Preparing for configurations

Scenario

When the network is congested, you wish to restrict burst flow on an interface, a VLAN, or some interface+VLAN to make it transmit in a well-proportioned rate to remove network congestion. Then, you need to configure rate limiting based on the interface, VLAN or interface+VLAN.

Prerequisite

Created VLANs.

5.7.2 Configuring rate limiting based on interface

Configure rate limiting based on interface for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.

Step	Command	Description
2	`Qtech(config)#`**`rate-limit port-list`** *`port-list`* `{` **`both`** *`rate-value`* `[` *`burst-value`* `] |` **`egress`** *`rate-value`* `[` *`burst-value`* `] |` **`ingress`** *`rate-value`* `[` *`burst-value`* `] }`	Configure rate limiting based on interface.

5.7.3 Configuring rate limiting based on VLAN

Configure rate limiting based on VLAN for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`rate-limit vlan`** *`vlan-id rate-value burst-value`* `[` **`statistics`** `]`	(Optional) configure rate limiting based on VLAN.

5.7.4 Configuring rate limiting based on interface+VLAN

Configure rate limiting based on interface+VLAN for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`rate-limit vlan`** *`vlan-id`* **`port-list`** *`port-list`* `{` **`both`** `|` **`ingress`** `|` **`egress`** `}` *`rate-value`* `[` *`burst-value`* `]`	(Optional) configure rate limiting based on interface+VLAN.

5.7.5 Configuring rate limiting based on QinQ

Configure rate limiting based on QinQ for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`rate-limit double-tagging-vlan outer`** `{` *`outer-vlan-id`* `|` **`any`** `}` **`inner`** `{` *`inner-vlan-id`* `|` **`any`** `}` *`rate-value burst-value`* `[` **`statistics`** `]`	(Optional) configure rate limiting based on QinQ.

5.7.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show rate-limit port-list** [*port-list*]	Show configurations of rate limiting based on interface.
2	Qtech#**show rate-limit vlan**	Show configurations of rate limiting based on VLAN or QinQ.
3	Qtech#**show rate-limit vlan** [*vlan-id*] **port-list** [*port-list*]	Show configurations of rate limiting based on interface+VLAN.

5.8 Maintenance

Maintain the QSW-8200 series switch as below.

Command	Description
Qtech(config)#**clear service-policy statistics** [**egress** [**class-map** *class-map-name*] | **ingress** [**class-map** *class-map-name*] | **port-list** *port-id*]	Clear statistics of packets for QoS traffic policy.
Qtech(config)#**clear rate-limit statistics vlan** [*vlan-id*]	Clear statistics of lost packets due to VLAN rate limiting.

5.9 Configuring examples

5.9.1 Example for configuring congestion management

Networking requirements

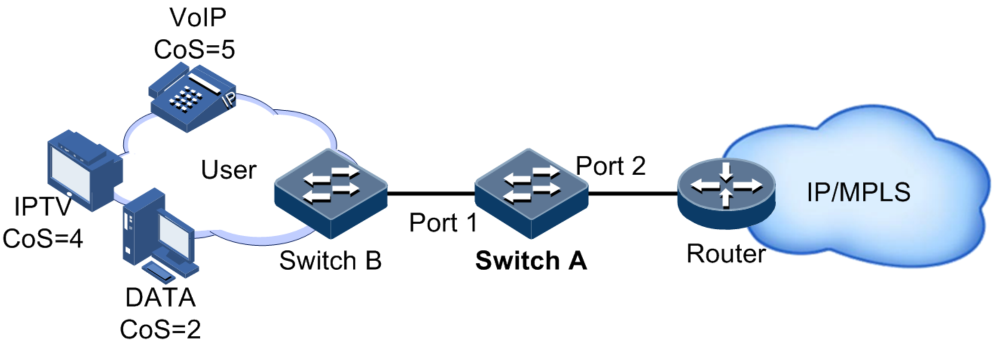
As shown in Figure 5-9, the user use voice, video and data services.

The CoS priority of voice service is 5, the CoS priority of video service is 4, and the CoS priority of data service is 2. The local priorities for these three types of services are mapping 6, 5, and 2 respectively.

Congestion can easily occur on Switch A. To reduce network congestion, make the following rules according to different services types:

- For voice service, perform SP schedule to make sure this part of flow passes through in precedence.
- For video service, perform WRR schedule, with weight value 50.
- For data service, perform WRR schedule, with weight value 20.

Figure 5-9 Queue scheduling networking



Configuration steps

Step 1 Configure interface priority trust mode.

```
Qtech#hostname SwitchA
SwitchA#config
SwitchA(config)#mls qos enable
SwitchA(config)#interface port 2
SwitchA(config-port)#mls qos trust cos
SwitchA(config-port)#quit
```

Step 2 Configure the profile for mapping between CoS priority and local priority.

```
SwitchA(config)#mls qos mapping cos-to-local-priority 1
SwitchA(cos-to-pri)#cos 5 to local-priority 6
SwitchA(cos-to-pri)#cos 4 to local-priority 5
SwitchA(cos-to-pri)#cos 2 to local-priority 2
SwitchA(cos-to-pri)#quit
```

Step 3 Apply the profile for mapping between CoS priority and local priority on port 2.

```
SwitchA(config)#interface port 2
SwitchA(config-port)#mls qos cos-to-local-priority 1
SwitchA(config-port)#quit
```

Step 4 Conduct SP+WRR queue scheduling in port 1 egress direction.

```
SwitchA(config)#interface port 1
SwitchA(config-port)#mls qos queue wrr 1 1 20 1 1 50 0 0
SwitchA(config-port)#quit
```

Checking results

Show priority trust mode on the interface.

```
Qtech#show mls qos port-list 1-28
Port      Priority   Trust-Mode  Scheduler-Mode
----------------------------------------------------
port1      0         Cos       SP
port2      0         Cos       SP
…
```

Show configurations of mapping between CoS priority and local priority

```
QtechA#show mls qos mapping cos-to-local-priority
G:GREEN
Y:Yellow
R:RED
cos-to-localpriority(color)
Index Description     CoS:  0     1    2    3    4    5   6     7
------------------------------------------------------------------------
1          localpri(color) :0(G)  1(G) 2(G) 3(G) 5(G) 6(G) 6(G) 7(G)
```

Show configurations of the profile for mapping between CoS priority and local priority on the interface.

```
SwitchA#show mls qos cos-to-local-priority port 2
Qtech#show mls qos cos-to-local-priority port-list 2
Port      CoS-To-Local-priority Profile Index
---------------------------------------------------
port2     1
```

Show configurations of queue scheduling on the interface.

```
Qtech#show mls qos queue port-list 1
port1
Queue    Weight(WRR)
-------------------------
  1      1
  2      1
  3      20
  4      1
  5      1
  6      50
  7      0
  8      0
…
```

5.9.2 Example for configuring rate limiting based on traffic policy

Networking requirements

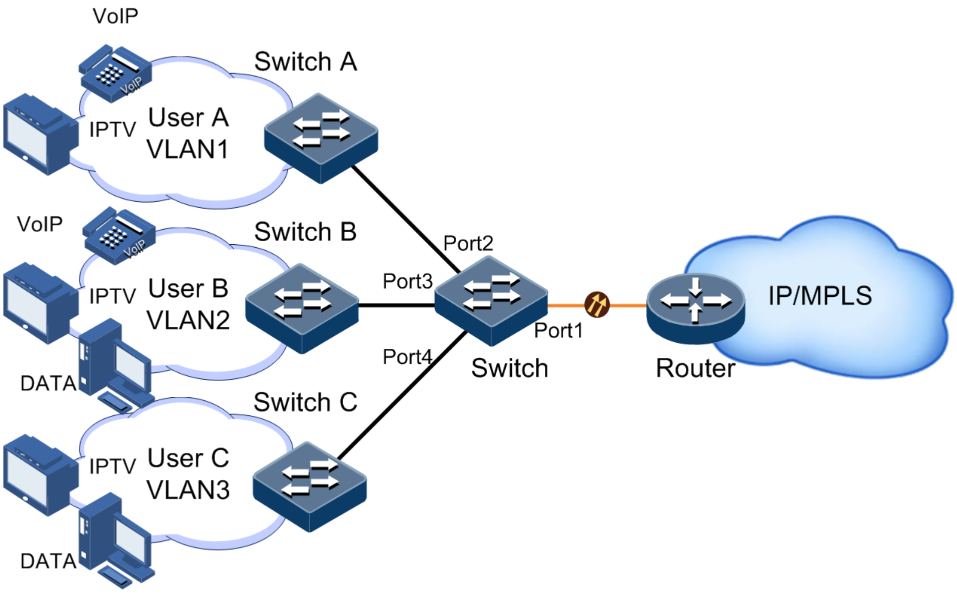
As show in Figure 5-10, User A, User B, and User C respectively belong to VLAN 1, VLAN 2, VLAN 3, and are connected to the Switch through Switch A, Switch B, Switch C.

User A uses voice and video services, User B provides voice, video and data services, and User C provides video and data services.

According to service requirements, user needs to make rules as below.

- For User A, provide 25 Mbit/s guaranteed bandwidth, permitting burst flow 100 KBytes and discarding redundant flow.
- For User B, provide 35 Mbit/s guaranteed bandwidth, permitting burst flow 100 KBytes and discarding redundant flow.
- For User C, provide 30 Mbit/s guaranteed bandwidth, permitting burst flow 100 KBytes and discarding redundant flow.

Figure 5-10 Rate limiting based on traffic policy



Configuration steps

Step 1 Create and configure traffic classification, classify different users according to VLAN ID.

```
Qtech#config
Qtech(config)#mls qos enable
Qtech(config)#class-map usera match-any
Qtech(config-cmap)#match vlan 1
Qtech(config-cmap)#quit
Qtech(config)#class-map userb match-any
Qtech(config-cmap)#match vlan 2
Qtech(config-cmap)#quit
Qtech(config)#class-map userc match-any
Qtech(config-cmap)#match vlan 3
Qtech(config-cmap)#quit
```

Step 2 Create rate limiting rules.

```
Qtech(config)#policer usera single
Qtech(traffic-policer)#cir 25000 cbs 100
Qtech(traffic-policer)#quit
Qtech(config)#policer userb single
Qtech(traffic-policer)#cir 35000 cbs 100
Qtech(traffic-policer)#quit
Qtech(config)#policer userc single
Qtech(traffic-policer)#cir 30000 cbs 100
Qtech(traffic-policer)#quit
```

Step 3 Create and configure traffic policy.

```
Qtech(config)#policy-map usera
Qtech(config-pmap)#class-map usera
Qtech(config-pmap-c)#police usera
Qtech(config-pmap-c)#quit
Qtech(config-pmap)#quit
Qtech(config)#service-policy usera egress 2
Qtech(config)#policy-map userb
Qtech(config-pmap)#class-map userb
Qtech(config-pmap-c)#police userb
Qtech(config-pmap-c)#quit
Qtech(config-pmap)#quit
Qtech(config)#service-policy userb egress 3
Qtech(config)#policy-map userc
Qtech(config-pmap)#class-map userc
Qtech(config-pmap-c)#police userc
Qtech(config-pmap-c)#quit
Qtech(config-pmap)#quit
Qtech(config)#service-policy userc egress 4
```

Checking results

Use the **show class-map** command to show configurations of traffic classification.

```
Qtech#show class-map usera
 Class Map match-any usera (id 0)
    Match vlan 1
Qtech#show class-map userb
 Class Map match-any userb (id 1)
    Match vlan 2
Qtech#show class-map userc
```

```
 Class Map match-any userb (id 2)
    Match vlan 3
```

Use the **show mls qos policer** command to show configurations of rate limiting rules.

```
Qtech(config)#show mls qos policer
single-policer usera  25000
 100
exceed-action drop
 Used by policy map usera
single-policer userb  35000
 100
exceed-action drop
 Used by policy map userb
single-policer userc  30000
 100
exceed-action drop
 Used by policy map userc
```

Use the **show policy-map** command to show configurations of traffic policy.

```
Qtech(config)#show policy-map
  Policy Map usera
    Class usera
        police usera

  Policy Map userb
    Class userb
        police userb

  Policy Map userc
    Class userc
        police userc
```

5.9.3 Example for configuring bandwidth guarantee based on interface

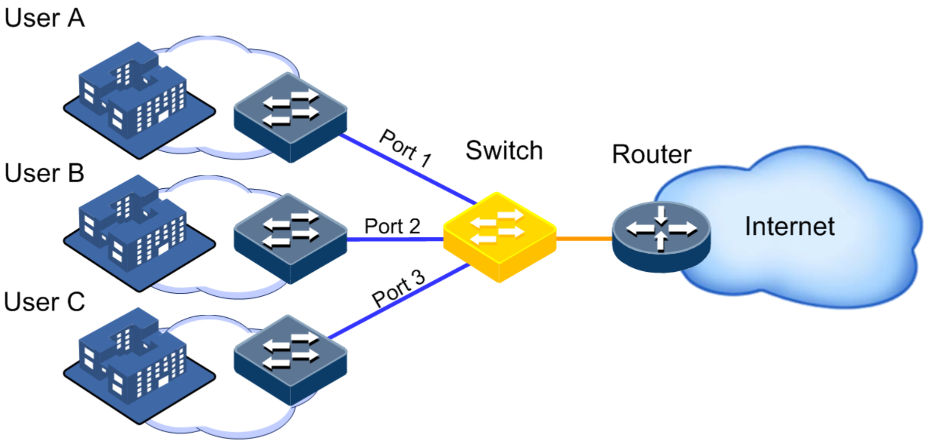
Networking requirements

Users A, B, and C have different service bandwidth requirements, as below.

- User A requires 25 Mbit/s guaranteed bandwidth, with 1 Mbit/s allowed excessive bandwidth, discarding rest bandwidth.
- User B requires 35 Mbit/s guaranteed bandwidth, with 1 Mbit/s allowed excessive bandwidth, discarding rest bandwidth.
- User C requires 30 Mbit/s guaranteed bandwidth, with 1 Mbit/s allowed excessive bandwidth, discarding rest bandwidth.

- To meet these users' requirements, configure bandwidth guarantee based on interface.

Figure 5-11 Networking with bandwidth guarantee based on interface



Configuration steps

Step 1 Create a bandwidth guarantee profile.

```
Qtech#config
Qtech(config)#bandwidth-profile 1 cir 25000 cbs 125 eir 1000 ebs 64
color-aware
Qtech(config)#bandwidth-profile 2 cir 35000 cbs 125 eir 1000 ebs 64
color-aware
Qtech(config)#bandwidth-profile 3 cir 30000 cbs 125 eir 1000 ebs 64
color-aware
```

Step 2 Apply the bandwidth guarantee profile to the specified interfaces.

```
Qtech(config)#bandwidth ingress port 1 1
Qtech(config)#bandwidth ingress port 2 2
Qtech(config)#bandwidth ingress port 3 3
```

Checking results

Use the **show bandwidth-profile** command to show configurations of the bandwidth guarantee profile.

```
Qtech#show bandwidth-profile all
BandwidthProfileIndex  Cir(kbps)  CBS(KB)  Eir(kbps)  EBS(KB)  Color-Mode
------------------------------------------------------------------------
1                      25000      125      1000       64       Color-Aware
2                      35000      125      1000       64       Color-Aware
3                      30000      125      1000       64       Color-Aware
```

Use the **show bandwidth port** *port-id* command to show configurations of bandwidth guarantee on the interface.

```
Qtech#show bandwidth port 1
Port    Direction   bwp-index   hv-bwp-index
---------------------------------------------------------------------------
3       Ingress     1          --
Qtech#show bandwidth port 2
Port    Direction   bwp-index   hv-bwp-index
---------------------------------------------------------------------------
4       Ingress     2          --
Qtech#show bandwidth port 3
Port    Direction   bwp-index   hv-bwp-index
---------------------------------------------------------------------------
5       Ingress     3          --
```

5.9.4 Example for configuring hierarchical bandwidth guarantee based on flow

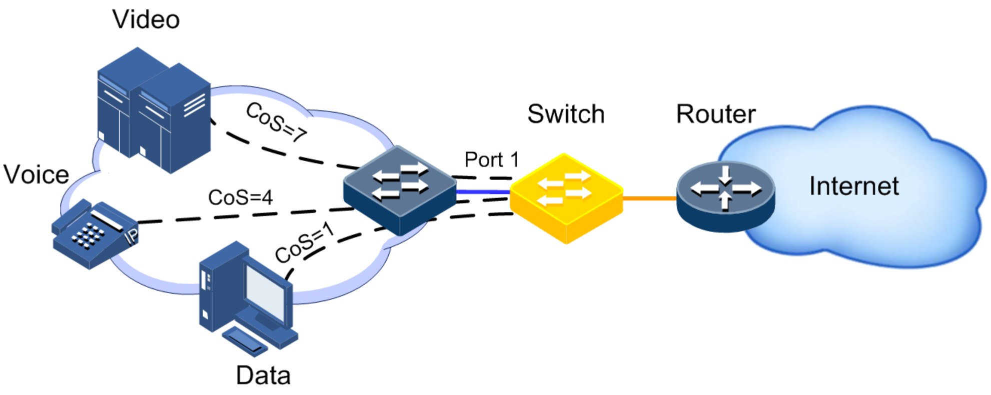
Networking requirements

As shown in Figure 5-12, a user uses video, voice, and data services with different bandwidth requirements as below.

- Video service: the guaranteed bandwidth is 5 Mbit/s, and the allowed excessive bandwidth is 5 Mbit/s, with rest bandwidth discarded.
- Voice service: the guaranteed bandwidth is 3 Mbit/s, and the allowed excessive bandwidth is 2 Mbit/s, with rest bandwidth discarded.
- Data service: the guaranteed bandwidth is 2 Mbit/s, and the allowed excessive bandwidth is 1 Mbit/s, with rest bandwidth discarded.

To meet user's requirements, configure hierarchical CoS bandwidth guarantee based on flow for video (CoS 7), voice (CoS 4), and data (CoS 1).

Figure 5-12 Networking with hierarchical bandwidth guarantee based on flow



Configuration steps

Step 1 Configure the bandwidth guarantee profile.

```
Qtech#config
Qtech(config)#bandwidth-profile 1 cir 5120 cbs 125 eir 5120 ebs 64 color-
aware
Qtech(config)#bandwidth-profile 2 cir 3072 cbs 125 eir 2048 ebs 64 color-
aware
Qtech(config)#bandwidth-profile 3 cir 2048 cbs 125 eir 1024 ebs 64 color-
aware
Qtech(config)#bandwidth-profile 4 cir 10240 cbs 125
```

Step 2 Configure the hierarchical CoS bandwidth guarantee profile.

```
Qtech(config)#hierarchy-cos bandwidth-profile 1
Qtech(config-hcos)#bandwidth coslist 7 1
Qtech(config-hcos)#bandwidth coslist 4 2
Qtech(config-hcos)#bandwidth coslist 1 3
Qtech(config-hcos)#exit
```

Step 3 Apply the hierarchical CoS bandwidth guarantee profile to ingress VLAN 2 packets from interface 1.

```
Qtech(config)#bandwidth ingress port 1 vlan 2 4 hierarchy-cos 1
```

Checking results

Use the **show bandwidth-profile** command to show configurations of the bandwidth guarantee profile.

```
Qtech#show bandwidth-profile all
BandwidthProfileIndex  Cir(kbps)  CBS(KB)  Eir(kbps)   EBS(KB)   Color-Mode
-------------------------------------------------------------------------
1                      5120       125      5120        64       Color-Aware
2                      3072       125      2048        64       Color-Aware
3                      2048       125      1024        64       Color-Aware
4                      10240      125      --          --       Color-Blind
```

Use the **show hierarchy-cos-bandwidth profile** command to show configurations of the hierarchical CoS bandwidth guarantee profile.

```
Qtech#show hierarchy-cos-bandwidth profile 1
```

```
hierarchy-cos bandwidth-profile 1
  bandwidth coslist 1  3
  bandwidth coslist 4  2
  bandwidth coslist 7  1
```

Use the **show bandwidth port** *port-id* **vlan** *vlan-id* command to show configurations of hierarchical CoS bandwidth guarantee on the interface.

```
Qtech#show bandwidth port 1 vlan 2
Port    Vlan    Coslist    Direction   bwp-index   hc-bwp-index
-------------------------------------------------------------------------
1       2        --        Ingress     4
```

5.9.5 Example for configuring rate limiting based on interface

Networking requirements

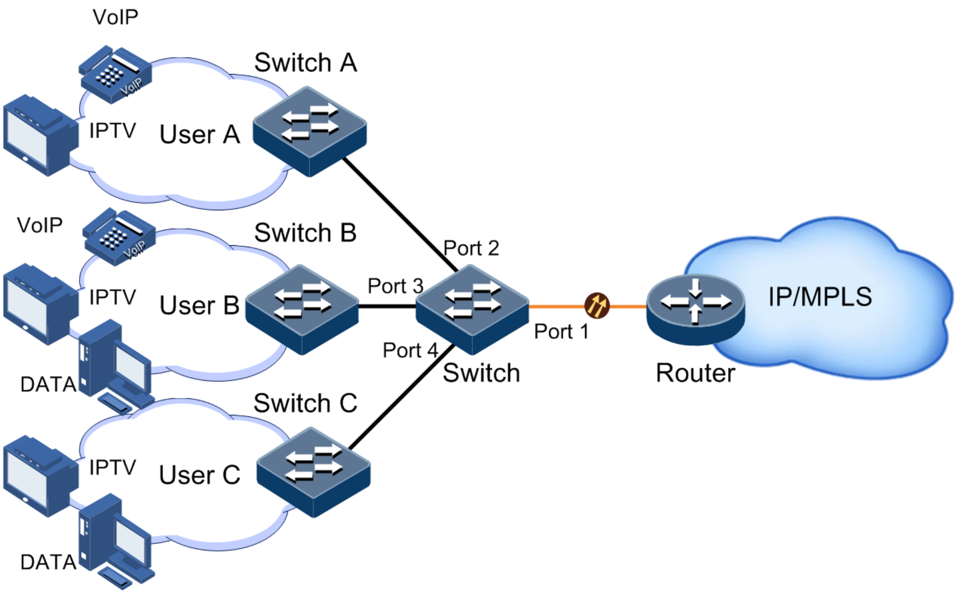
As shown in Figure 5-13, User A, User B, User C are respectively connected to Switch A, Switch B, Switch C, and the QSW-8200 series switch.

User A uses voice and video services. User B uses voice, video and data services. User C uses video and data services.

According to service requirements, make rules as below.

- For User A, provide 25 Mbit/s guaranteed bandwidth, permitting burst flow 100 KBytes and discarding redundant flow;
- For User B, provide 35 Mbit/s guaranteed bandwidth, permitting burst flow 100 KBytes and discarding redundant flow;
- For User C, provide 30 Mbit/s guaranteed bandwidth, permitting burst flow 100 KBytes and discarding redundant flow.

Figure 5-13 Rate limiting based on interface



Configuration steps

Step 1 Configure rate limiting based on interface.

```
Qtech#config
Qtech(config)#rate-limit port-list 2 ingress 25000 100
Qtech(config)#rate-limit port-list 3 ingress 35000 100
Qtech(config)#rate-limit port-list 4 ingress 30000 100
```

Checking results

Use the **show rate-limit port-list** command to show configurations of rate limiting based on interface.

```
Qtech(config)#show rate-limit port-list 2-4
I-Rate:  Ingress Rate
I-Burst: Ingress Burst
E-Rate:  Egress Rate
E-Burst: Egress Burst

Port     I-Rate(kbps)   I-Burst(kB)   E-Rate(kbps)   E-Burst(kB)
----------------------------------------------------------------------
P2          25000          100          3448            34
P3          35000          100          3448            34
P4          30000          100       1048576            512
```

6 Multicast

This chapter describes basic principle and configuration of multicast and provides related configuration examples, including the following sections:

- Overview
- Configuring IGMP basis
- Configuring IGMP Snooping
- Configuring MVR
- Configuring MVR Proxy
- Configuring IGMP filtering
- Multicast VLAN copy
- Configuration examples

6.1 Overview

With the continuous development of Internet, more and more various interactive data, voice, and video emerge on the network. On the other hand, the emerging e-commerce, online meetings, online auctions, video on demand, remote learning, and other services also rise gradually. These services come up with higher requirements for network bandwidth, information security, and paid feature. Traditional unicast and broadcast cannot meet these requirements well, while multicast has met them timely.

Multicast is a point-to-multipoint data transmission method. The method can effectively solve the single point sending and multipoint receiving problems. During transmission of packets on the network, multicast can save network resources and improve information security.

Comparison among unicast, broadcast and multicast

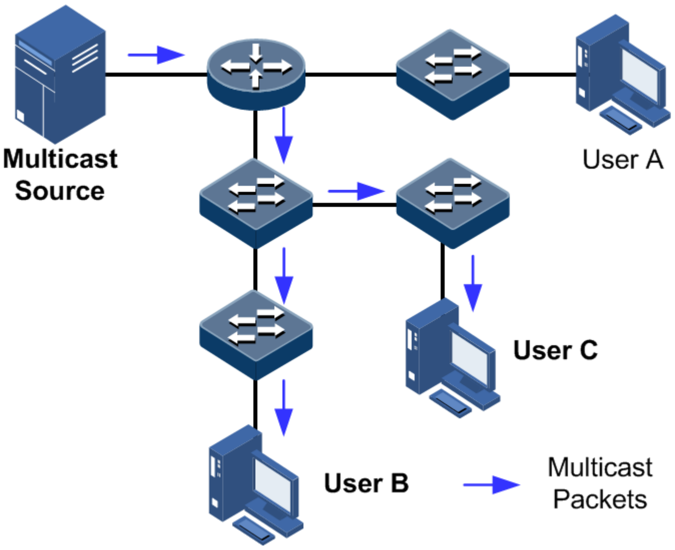
Multicast is a kind of packets transmission method which is parallel with unicast and broadcast.

- Unicast: the system establishes a data transmission path for each user who needs the information, and sends separate copy information about them. Through unicast, the amount of information transmitted over the network is proportional to the number of users, so when the number of users becomes huge, there will be more identical information on the network. In this case, bandwidth will become an important bottleneck, and unicast will not be conducive to large-scale information transmission.

- Broadcast: the system sends information to all users regardless of whether they need or not, so any user will receive it. Through broadcast, the information source delivers information to all users in the network segment, which fails to guarantee information security and paid service. In addition, when the number of users who require this kind of information decreases, the utilization of network resources will be very low, and the bandwidth will be wasted seriously.
- Multicast: when some users in the network need specific information, the sender only sends one piece of information, then the transmitted information can be reproduced and distributed in fork junction as far as possible.

As shown in Figure 6-1, assume that User B and User C need information, you can use multicast transmission to combine User B and User C to a receiver set, then the information source just needs to send one piece of information. Each switch on the network will establish their multicast forwarding table according to IGMP packets, and finally transmits the information to the actual receiver User B and User C.

Figure 6-1 Multicast transmission networking



In summary, the unicast is for a network with sparse users and broadcast is for a network with dense users. When the number of users in the network is uncertain, unicast and broadcast will present low efficiency. When the number of users are doubled and redoubled, the multicast mode does not need to increase backbone bandwidth, but sends information to the user in need. These advantages of multicast make itself become a hotspot in study of the current network technology.

Advantages and application of multicast

Compared with unicast and broadcast, multicast has the following advantages:

- Improve efficiency: reduce network traffic, relieve server and CPU load.
- Optimize performance: reduce redundant traffic and guarantee information security.
- Support distributed applications: solve the problem of point-point data transmission.

The multicast technology is used in the following aspects:

- Multimedia and streaming media, such as, network television, network radio, and real-time video/audio conferencing

- Training, cooperative operations communications, such as: distance education, telemedicine
- Data warehousing, financial applications (stock)
- Any other "point-to-multipoint" applications

Basic concepts in multicast

- Multicast group

A multicast group refers to the recipient set using the same IP multicast address identification. Any user host (or other receiving device) will become a member of the group after joining the multicast group. They can identify and receive multicast data with the destination address as IP multicast address.

- Multicast group members

Each host joining a multicast group will become a member of the multicast group. Multicast group members are dynamic, and hosts can join or leave multicast group at any time. Group members may be widely distributed in any part of the network.

- Multicast source

A multicast source refers to a server which regards multicast group address as the destination address to send IP packet. A multicast source can send data to multiple multicast groups; multiple multicast sources can send to a multicast group.

- Multicast router

A multicast router is a router that supports Layer 3 multicast. The multicast router can achieve multicast routing and guide multicast packet forwarding, and provide multicast group member management to distal network segment connecting with users.

- Router interface

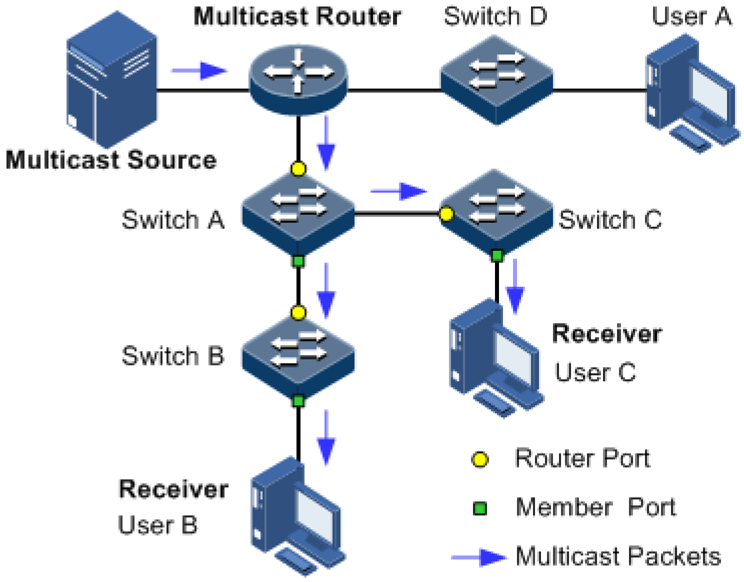
A router interface refers to the interface toward multicast router between a multicast router and a host. The QSW-8200 series switch receives multicast packets from this interface.

- Member interface

Known as the receiving interface, a member interface is the interface towards the host between multicast router and the host. The QSW-8200 series switch sends multicast packets from this interface.

Figure 6-2 shows basic concepts in multicast.

Figure 6-2 Basic concepts in multicast



Multicast address

To make multicast source and multicast group members communicate across the Internet, you need to provide network layer multicast address and link layer multicast address, namely, the IP multicast address and multicast MAC address.

- IP multicast address

Internet Assigned Numbers Authority (IANA) assigns Class D address space to IPv4 multicast; the IPv4 multicast address ranges from 224.0.0.0 to 239.255.255.255.

- Multicast MAC address

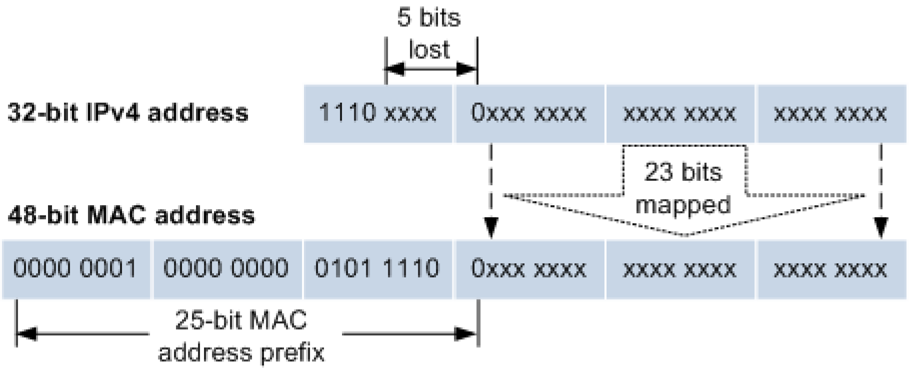
When the Ethernet transmits unicast IP packets, it uses the MAC address of the receiver as the destination MAC address. However, when multicast packets are transmitted, the destination is no longer a specific receiver, but a group with an uncertain number of members, so the Ethernet needs to use the multicast MAC address.

The multicast MAC address identifies receivers of the same multicast group on the link layer.

According to IANA, high bit 24 of the multicast MAC address are 0x01005E, bit 25 is fixed to 0, and the low bit 23 corresponds to low bit 23 of the IPv4 multicast address.

Figure 6-3 shows mapping between the IPv4 multicast address and MAC address.

Figure 6-3 Mapping between IPv4 multicast address and multicast MAC address



The first 4 bits of IP multicast address are 1110, indicating multicast identification. In the last 28 bits, only 23 bits are mapped to the multicast MAC address, and the missing of 5 bits makes 32 IP multicast addresses mapped to the same multicast MAC address. Therefore, in Layer 2, the QSW-8200 series switch may receive extra data besides IPv4 multicast group, and these extra multicast data needs to be filtered by the upper layer on the QSW-8200 series switch.

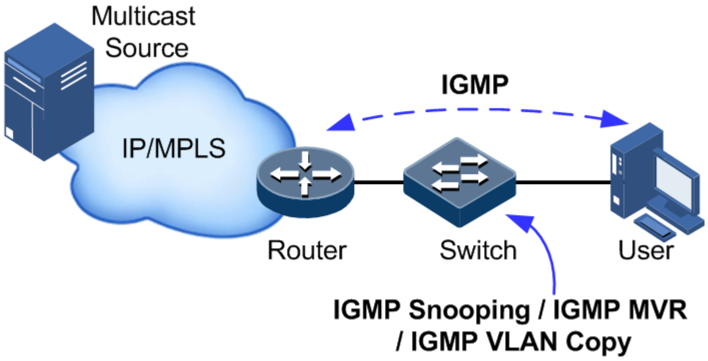
Basis of multicast protocol

To implement complete set of multicast services, you need to deploy a variety of multicast protocols in various positions of network and make them cooperate with each other.

Typically, IP multicast working at network layer is called Layer 3 multicast, so the corresponding multicast protocol is called Layer 3 multicast protocol, including Internet Group Management Protocol (IGMP). IP multicast working at data link layer is called Layer 2 multicast, so the corresponding multicast protocol is called Layer 2 multicast protocol, including Internet Group Management Protocol (IGMP) Snooping.

Figure 6-4 shows operating of IGMP and Layer 2 multicast features.

Figure 6-4 Operating of IGMP and Layer 2 multicast features



IGMP, a protocol in TCP/IP protocol suite, is responsible for managing IPv4 multicast members. IGMP runs between the multicast router and host, defines the establishment and maintenance mechanism of multicast group membership between hosts and the multicast router. IGMP is not involved in transmission and maintenance of group membership between multicast routers, which is completed by the multicast routing protocol.

IGMP manages group members through interaction of IGMP packets between the host and multicast router. IGMP packets are encapsulated in IP packets, including Query packets, Report packets, and Leave packets. Basic functions of IGMP are as below:

- The host sends Report packets to join the multicast group, sends Leave packets to leave the multicast group, and automatically decides which multicast group packets to receive.
- The multicast router sends Query packets periodically, and receives Report packets and Leave packets from hosts to understand the multicast group members in connected network segment. The multicast data will be forwarded to the network segment if there are multicast group members, and not forward if there are no multicast group members.

Up to now, IGMP has three versions: IGMPv1, IGMPv2, and IGMPv3. The newer version is fully compatible with the elder version. Currently the most widely used version is IGMPv2, while the Leave packet does not IGMPv1.

Layer 2 multicast runs on Layer 2 devices between the host and multicast router.

Layer 2 multicast manages and controls multicast groups by monitoring and analyzing IGMP packets exchanged between hosts and multicast routers to implement forwarding multicast data at Layer 2 and suppress multicast data diffusion at Layer 2.

Supported multicast features

The QSW-8200 series switch supports the following multicast features:

- Basic IGMP functions
- Internet Group Management Protocol Snooping (IGMP) Snooping
- Multicast VLAN Registration (MVR)
- MVR Proxy
- IGMP filtering

Note

- IGMP Snooping and IGMP MVR can be concurrently enabled on the QSW-8200 series switch.
- The QSW-8200 series switch supports both IGMPv1 and IGMPv2.

6.1.2 Basic IGMP functions

Basic IGMP functions are as below:

- Assign the multicast router interface.
- Enable immediate leaving.
- Set multicast forwarding entries and the aging time of router interfaces.
- Enable IGMP ring network forwarding.

Basic functions of Layer 2 multicast provide Layer 2 multicast common features, which must be used on the QSW-8200 series switch enabled with IGMP Snooping or IGMP MVR.

Note

Configurations of basic function take effect on IGMP Snooping or IGMP MVR concurrently.

The concepts related to IGMP basic functions are as below.

Multicast router interface

The router interface can be learnt dynamically (learnt through IGMP query packets, on the condition that the multicast routing protocol is enabled on multicast routers) on Layer 2 multicast switch, or set manually to forward downstream multicast report and leave packets to the router interface.

The router interface learnt dynamically has an aging time, while the router interface configured manually will not be aged.

Aging time

The configured aging time takes effect on both multicast forwarding entries and the router interface.

On Layer 2 switch running multicast function, each router interface learnt dynamically starts a timer, of which the expiration time is the aging time of IGMP Snooping. The router interface will be deleted if no IGMP Query packets are received in the aging time. The timer of the router interface will be updated when an IGMP Query packet is received.

Each multicast forwarding entry starts a timer, namely, the aging time of a multicast member. The expiration time is IGMP Snooping aging time. The multicast member will be deleted if no IGMP Report packets are received in the aging time. Update timeout for multicast forwarding entry when receiving IGMP Report packets. The timer of the multicast forwarding entry will be updated when an IGMP Report packet is received.

Immediate leaving

On Layer 2 switch running multicast function, the system will not delete the corresponding multicast forwarding entry immediately, but wait until the entry is aged after sending Leave packets. Enable this function to delete the corresponding multicast forwarding entry quickly when there are a large number of downstream users and adding or leaving is more frequently required.

Note

Only IGMPv2/v3 version supports immediate leaving.

IGMP ring network forwarding

On Layer 2 switch running multicast function, IGMP ring network forwarding can be enabled on any type of interfaces.

Enabling IGMP ring network forwarding can implement multicast backup protection on the ring network, make multicast services more stable, and prevent link failure from causing multicast service failure.

IGMP ring network forwarding can be applied to the Ethernet ring, STP/RSTP/MSTP ring, and G.8032 ring, etc.

6.1.3 IGMP Snooping

IGMP Snooping is a multicast constraining mechanism running on Layer 2 devices, used for managing and controlling multicast groups, and implementing Layer 2 multicast.

IGMP Snooping allows the QSW-8200 series switch to monitor IGMP session between the host and multicast router. When monitoring a group of IGMP Report from host, the QSW-8200 series switch will add host-related interface to the forwarding entry of this group. Similarly, when a forwarding entry reaches the aging time, the QSW-8200 series switch will delete host-related interface from forwarding entry.

IGMP Snooping forwards multicast data through Layer 2 multicast forwarding entry. When receiving multicast data, the QSW-8200 series switch will forward them directly according to the corresponding receiving interface of the multicast forwarding entry, instead of flooding them to all interfaces, to save bandwidth of the QSW-8200 series switch effectively.

IGMP Snooping establishes a Layer 2 multicast forwarding table, of which entries can be learnt dynamically or configured manually.

Note

Currently, the QSW-8200 series switch supports up to 1024 Layer 2 multicast entries.

6.1.4 MVR

Multicast VLAN Registration (MVR) is multicast constraining mechanism running on Layer 2 devices, used for multicast group management and control and achieve Layer 2 multicast.

MVR adds member interfaces belonging to different customer VLANs on the Layer device to multicast VLAN by configuring multicast VLAN and makes different VLAN user uses one common multicast VLAN, then the multicast data will be transmitted only in one multicast VLAN without copying one for each customer VLAN, thus saving bandwidth. At the same time, multicast VLAN and customer VLAN are completely isolated which also increases the security.

Both MVR and IGMP Snooping can achieve Layer 2 multicast, but the difference is: multicast VLAN in IGMP Snooping is the same with customer VLAN, while multicast VLAN in MVR can be different with customer VLAN.

Note

One switch can be configured with up to 10 multicast VLAN, at least one multicast VLAN and group addresses. It supports up to 1024 multicast groups.

6.1.5 MVR Proxy

MVR Proxy is an MVR protocol proxy mechanism. It runs on Layer 2 devices to assist in managing and controlling multicast groups. MVR Proxy will terminate IGMP packets. It can proxy host function and also proxy multicast router functions for the next agent. The Layer 2 network device enabled with MVR Proxy has two roles:

- On the user side, it is a query builder and undertakes the role of Server, sending Query packets and periodically checking user information, and dealing with the Report and Leave packets from user.
- On the network routing side, it is a host and undertakes the role of Client, responding the multicast router Query packet and sending Report and Leave packets. It sends the user information to the network when they are in need.

The proxy mechanism can control and access user information effectively, at the same time, reducing the network side protocol packet and network load.

MVR Proxy establishes the multicast forwarding table by blocking IGMP packets between users and the multicast router.

Note

MVR Proxy is usually used with MVR.

The following concepts are related to MVR Proxy.

- IGMP packet suppression

IGMP packet suppression refers that the Layer 2 device filters identical Report packets. When receiving Report packets from a multicast group member in a query interval, the Layer 2 device sends the first Report packet to the multicast router only rather than other identical Report packets, to reduce packet quantity on the network.

Note

When MVR is enabled, IGMP packet suppression can be enabled or disabled respectively.

- IGMP Querier

If a Layer 2 device is enabled with this function, it can actively send IGMP query packets to query information about multicast members on the interface. If it is disabled with this function, it only forwards IGMP query packets from routers.

Note

When IGMP Snooping is enabled, IGMP Querier can be enabled or disabled respectively.

- Source IP address of query packets sent by IGMP Querier

IGMP querier sends the source IP address of query packets. By default, the IP address of IP interface 0 is used. If the IP address is not configured, 0.0.0.0 is used. When receiving query packets with IP address of 0.0.0.0, some hosts take it illegal and do not respond. Thus, specifying the IP address for the query packet is recommended.

- Query interval

It is the query interval for common groups. The query message of common group is periodically sent by the Layer 2 device in multicast mode to all hosts in the shared network segment, to query which multicast groups have members.

- Maximum response time for query packets

The maximum response time for query packets is used to control the deadline for reporting member relations by a host. When the host receives query packets, it starts a timer for each added multicast group. The value of the timer is between 0 and maximum response time. When the timer expires, the host sends the Report packet to the multicast group.

- Interval for last member to send query packets

It is also called the specified group query interval. It is the interval for the Layer 2 device continues to send query packets for the specified group when receiving IGMP Leave packet for a specified group by a host.

The query packet for the specified multicast group is sent to query whether the group has members on the interface. If yes, the members must send Report packets within the maximum response time; after the Layer 2 device receives Report packets in a specie period, it continues to maintain multicast forwarding entries of the group; If the members fail to send Report packets within the maximum response time, the switch judges that the last member of the multicast group has left and thus deletes multicast forwarding entries.

6.1.6 IGMP filtering

To control user access, you can set IGMP filtering. IGMP filtering contains the range of accessible multicast groups passing filtering rules and the maximum number of groups.

- IGMP filtering rules

To ensure information security, the administrator needs to limit the multicast users, such as what multicast data are allowed to receive and what are not.

Configure IGMP Profile filtering rules to control the interface. One IGMP Profile can be set one or more multicast group access control restrictions and access the multicast group according to the restriction rules (**permit** and **deny**). If a rejected IGMP Profile filter profile is applied to the interface, the interface will discard the IGMP report packet from this group directly once receiving it and does not allow receiving this group of multicast data.

IGMP filtering rules can be configured on an interface or VLAN.

IGMP Profile only applies to dynamic multicast groups, but not static ones.

- Limit to the maximum number of multicast groups

The maximum allowed adding number of multicast groups and the maximum group limitation rule can be set on an interface or interface+VLAN.

The maximum group limitation rule sets the actions for reaching the maximum number of multicast group users added, which can be no longer allowing user adding groups, or covering the original adding group.

Note

IGMP filtering is usually used with MVR.

6.2 Configuring IGMP basis

6.2.1 Configuring basic IGMP functions

Configure basic IGMP functions for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**igmp mrouter vlan** *vlan-id interface-type interface-number*	(Optional) configure multicast route interface.
3	Qtech(config)#**igmp immediate-leave** *interface-type interface-number* [**vlan** *vlan-list*]	(Optional) configure immediate leaving on the interface+VLAN.

Step	Command	Description
4	`Qtech(config)#igmp timeout { period | infinite }`	(Optional) configure the aging time of multicast forwarding entries. The aging time configured takes effect on all dynamically learnt router interfaces and multicast forwarding entries.
5	`Qtech(config)#igmp ring interface-type interface-number`	(Optional) enable IGMP ring network forwarding on the interface.
6	`Qtech(config)#mac-address-table static multicast mac-address vlan vlan-id interface-type interface-number-list`	(Optional) configure the interface to join static multicast group. An interface is added to the multicast group through the IGMP Report packet send by a host. You can also manually add it to a multicast group.

6.2.2 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Qtech#show igmp mrouter`	Show configurations of the multicast route interface.
2	`Qtech#show igmp immediate-leave [ interface-type interface-number ]`	Show configuration of immediate leaving on Layer 2 multicast.
3	`Qtech#show igmp statistics [ interface-type interface-number ]`	Show Layer 2 multicast statistics.

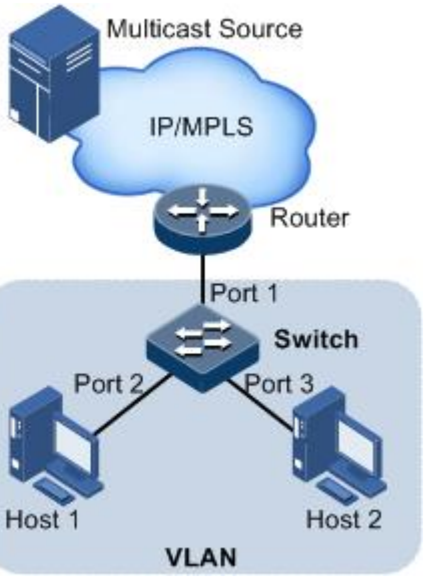
6.3 Configuring IGMP Snooping

6.3.1 Preparing for configurations

Scenario

As shown in Figure 6-5, multiple hosts belonging to the same VLAN receive data from the multicast source. Enable IGMP Snooping on the Layer 2 device that connects the multicast router and hosts. By listening IGMP packets transmitted between the multicast router and hosts, creating and maintaining the multicast forwarding table, you can implement Layer 2 multicast.

Figure 6-5 IGMP Snooping networking



Prerequisite

Create a VLAN, and add related interfaces to the VLAN.

6.3.2 Default configurations of IGMP Snooping

Default configurations of IGMP Snooping are as below.

Function	Default value
Global IGMP Snooping status	Disable
VLAN IGMP Snooping status	Disable

6.3.3 Configuring IGMP Snooping

Configure IGMP Snooping for the QSW-8200 series switch as below.

Step	Function	Default value
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`igmp snooping`**	Enable global IGMP Snooping.
3	`Qtech(config)#`**`igmp snooping vlan`** *`vlan-list`*	Enable IGMP Snooping in the VLAN.

Step	Function	Default value
4	Qtech(config)#**mac-address-table static multicast** *mac-address* **vlan** *vlan-id interface-type interface-number-list*	(Optional) configure the interface to join static multicast group. An interface is added to the multicast group through the IGMP Report packet send by a host. You can also manually add it to a multicast group

6.3.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show igmp snooping** [**vlan** *vlan-list*]	Show configurations of IGMP Snooping.
2	Qtech#**show igmp snooping member** [*interface-type interface-number* | **vlan** *vlan-id*]	Show information about multicast members of IGMP Snooping.

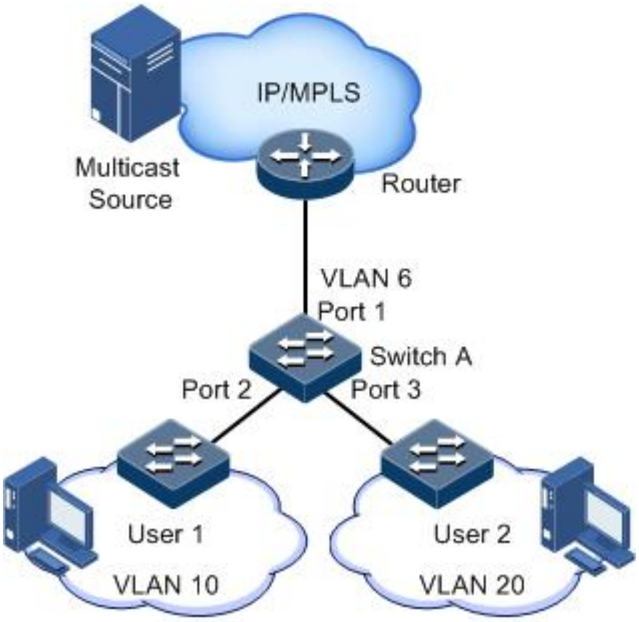
6.4 Configuring MVR

6.4.1 Preparing for configurations

Scenario

As shown in Figure 6-6, multiple hosts receive data from the multicast sources. These hosts and the multicast router belong to different VLANs. Enable MVR on Switch A, and configure multicast VLAN. In this way, users in different VLANs can share a multicast VLAN to receive the same multicast data, and bandwidth waste is reduced.

Figure 6-6 IGMP MVR networking



Prerequisite

Create VLANs and add related interfaces to VLANs.

6.4.2 Default configurations of MVR

Default configurations of MVR are as below.

Function	Default value
Global IGMP MVR status	Disable
Interface IGMP MVR status	Disable
Multicast VLAN and group address set	N/A

6.4.3 Configuring MVR basic information

Configure MVR basic information about QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`igmp mvr`**	Enable global IGMP MVR.
3	`Qtech(config)#`**`igmp mvr`** *`interface-type interface-number`*	Enable interface IGMP MVR.

Step	Command	Description
4	Qtech(config)#**igmp mvr mcast-vlan** *vlan-id* **group** { *start-ip-address* [*end-ip-address*] | **any** }	Configure group address set for multicast VLAN. Note After IGMP MVR is enabled, you need to configure multicast VLAN and bind group address set. If the received IGMP Report packet does not belong to a group address set of any VLAN, it is not processed and the user cannot make multicast traffic on demand.
5	Qtech(config)#**mac-address-table static multicast** *mac-address* **vlan** *vlan-id interface-type interface-number-list*	(Optional) configure static multicast forwarding table. An interface is added to the multicast group through the IGMP Report packet send by a host. You can also manually add it to a multicast group.

6.4.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show igmp mvr**[*interface-type interface-number*]	Show configurations of IGMP MVR.
2	Qtech#**show igmp mvr member** [*interface-type interface-number* | **user-vlan** *vlan-id*]	Show information about MVR multicast member.
3	Qtech#**show igmp mvr vlan-group** [**mcast-vlan** *vlan-id*]	Show MVR multicast VLAN and group address set.

6.5 Configuring MVR Proxy

6.5.1 Preparing for configurations

Scenario

In a network with multicast routing protocol widely applied, there are multiple hosts and client subnet receiving multicast information. Enable IGMP Proxy on the Layer 2 device that connects the multicast router and hosts, to block IGMP packets between hosts and the multicast router and relieve the network load.

Configure IGMP Proxy to relive configuration and management of client subnet for the multicast router and to implement multicast connection with the client subnet.

IGMP Proxy is usually used in cooperation with IGMP Snooping or IGMP MVR.

Prerequisite

Create a VLAN, and add related interfaces into it.

6.5.2 Default configurations of IGMP Proxy

Default configurations of IGMP Proxy are as below.

Function	Default value
IGMP Proxy status	Disable
IGMP packet suppression status	Disable
IGMP Querier status	Disable
Source IP address for IGMP Querier and IGMP Proxy to send packets	Use the IP address of IP interface 0. If IP interface 0 is not configured, use 0.0.0.0.
IGMP query interval	60s
Maximum response time to send Query packets	10s
Interval for the last member to send Query packets	1s

6.5.3 Configuring IGMP Proxy

Configure IGMP Proxy for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`igmp proxy`**	Enable IGMP Proxy.
3	`Qtech(config)#`**`igmp proxy suppression`**	Enable IGMP packet suppression.
4	`Qtech(config)#`**`igmp proxy querier`**	(Optional) enable IGMP querier.
5	`Qtech(config)#`**`igmp proxy source-ip`** *`ip-address`*	(Optional) configure the source IP address for the IGMP querier to send query packets.
6	`Qtech(config)#`**`igmp proxy query-interval`** *`seconds`*	(Optional) configure the IGMP query interval.
7	`Qtech(config)#`**`igmp proxy query-max-response-time`** *`period`*	(Optional) configure the maximum response time to send query packets.
8	`Qtech(config)#`**`igmp proxy last-member-query`** *`period`*	(Optional) configure the interval for the last member to send query packets.

Note

- When IGMP Proxy is disabled, the following parameters of MVR Proxy can be configured: source IP address, query interval, maximum response time to send Query packets, and interval for the last member to send Query packets. After IGMP Proxy is enabled, these configurations will take effect immediately.
- IGMP Proxy can be enabled when IGMP Snooping or IGMP MVR is enabled.

6.5.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Qtech#show mvr proxy`	Show configurations of IGMP Proxy.

6.6 Configuring IGMP filtering

6.6.1 Preparing for configurations

Scenario

Different users in the same multicast group receive different multicast requirements and permissions, and allow configuring filtering rules on the switch which connects multicast router and user host to restrict multicast users.

The maximum number of multicast groups allowed for users to join can be set.

IGMP filtering is used in cooperation with IGMP Snooping or IGMP MVR.

Prerequisite

Create a VLAN, and add related interfaces into it.

6.6.2 Default configurations of IGMP filtering

Default configurations of IGMP filtering are as below.

Function	Default value
Global IGMP filtering	Disable
IGMP filter profile Profile	N/A
IGMP filter profile action	Refuse
IGMP filtering on the interface	No maximum group limit. The largest group action is drop, and no application filter profile.
IGMP filtering under interface+VLAN	No maximum group limit. The largest group action is drop, and there is no application filter profile.

6.6.3 Enabling global IGMP filtering

Enable global IGMP filtering for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode
2	Qtech(config)#**igmp filter**	Enable global IGMP filtering

Note

Before configuring IGMP filter profile or the maximum number of IGMP groups, use the **igmp filter** command to enable global IGMP filtering.

6.6.4 Configuring IGMP filtering rules

IGMP filtering rules can be used on an interface or on the interface+VLAN.

Configure the IGMP filter profile for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode
2	Qtech(config)#**igmp filter profile** *profile-number*	Create IGMP Profile and enter Profile configuration mode.
3	Qtech(config-igmp-profile)#**permit** | **deny**	Configure IGMP Profile action.
4	Qtech(config-igmp-profile)#**range** *range-id start-ip-address* [*end-ip-address*]	Configure to control IP multicast address access and range.
5	Qtech(config-igmp-profile)#**exit** Qtech(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode or LAG configuration mode.
6	Qtech(config-port)#**igmp filter profile** *profile-number* [**vlan** *vlan-list*]	Configure IGMP Profile filter profile to physical interface or interface+VLAN.
	Qtech(config-aggregator)#**igmp filter profile** *profile-number* [**vlan** *vlan-list*]	Configure IGMP Profile filter profile to LAG interface or interface+VLAN.

Note

Perform the command of **igmp filter profile** *profile-number* in interface configuration mode to make the created IGMP Profile apply to the specified interface. One IGMP

Profile can be applied to multiple interfaces, but each interface can have only one IGMP Profile.

6.6.5 Configuring maximum number of multicast groups

You can add the maximum number of multicast groups applied to interface or interface+VLAN.

Configuring maximum number of multicast groups on interface

Configure the maximum number of multicast groups on the interface for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode
2	Qtech(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode or LAG configuration mode.
3	Qtech(config-port)#**igmp filter max-groups** *group-number* [**vlan** *vlan-list*]	Configure the maximum number of multicast groups to physical interface or interface+VLAN.
	Qtech(config-aggregator)#**igmp filter max-groups** *group-number* [**vlan** *vlan-list*]	Configure the maximum number of multicast groups to LAG interface or interface+VLAN.
4	Qtech(config-port)#**igmp filter max-groups action** { **drop** | **replace** } [**vlan** *vlan-list*]	(Optional) configure the action to take when the number of physical interfaces or interface+VLANs exceeds the maximum number of multicast groups.
	Qtech(config-aggregator)#**igmp filter max-groups action** { **drop** | **replace** } [**vlan** *vlan-list*]	(Optional) configure the action to take when the number of LAG interfaces or interface+VLANs exceeds the maximum number of multicast groups.

6.6.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show igmp filter** [**interface** | *interface-type interface-number* [**vlan** *vlan-id*]]	Show configurations of IGMP filtering.
2	Qtech#**show igmp filter profile** [*profile-number*]	Show configurations of IGMP Profile.

6.7 Multicast VLAN copy

6.7.1 Preparing for configurations

Scenario

When the VLAN of multicast data flow and the user to apply for the multicast data flow are in different VLANs, the user cannot obtain the multicast data flow. Multicast VLAN copy can solve this problem. After multicast VLAN copy is enabled, the QSW-8200 series switch writes the mapping between the customer VLAN and the VLAN of the multicast data flow to be applied for in a forwarding table when it receives a request from the user to access the multicast data flow. When receiving the multicast data flow, the QSW-8200 series switch copies the multicast data flow to each customer VLAN according to the forwarding table.

Prerequisite

Disable IGMP Snooping/IGMP MVR.

6.7.2 Default configurations of multicast VLAN copy

Default configurations of multicast VLAN copy are as below.

Function	Default value
Global multicast VLAN copy status	Disable
Interface multicast VLAN copy status	Disable
Static forwarding table of multicast VLAN copy	N/A
Binding of multicast LAN and multicast group	N/A

6.7.3 Configuring multicast VLAN copy

Configure multicast VLAN copy for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**igmp vlan-copy**	Enable global multicast VLAN copy.
3	Qtech(config)#**igmp vlan-copy port-list** *port-list*	Enable interface multicast VLAN copy.
4	Qtech(config)#**igmp vlan-copy mcast-vlan** *vlan-list* **group** { *start-ip-address* [*end-ip-address*] | **any** }	Configure binding of multicast LAN and multicast group.
5	Qtech(config)#**igmp vlan-copy static vlan** *vlan-id* **group** *ip-address interface-type interface-number* **copy-vlan-list** *vlan-list*	(Optional) configure the static forwarding table of multicast VLAN copy.

6.7.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show igmp vlan-copy** [*interface-type interface-number*]	Show configurations of multicast VLAN copy on the specified interface or globally.
2	Qtech#**show igmp vlan-copy interface**	Show multicast VLAN copy status on each interface.
3	Qtech#**show igmp vlan-copy member** [*interface-type interface-number* | **user-vlan** *vlan-list*]	Show information about dynamically learnt multicast groups of multicast VLAN copy by the QSW-8200 series switch.
4	Qtech#**show igmp vlan-copy vlan-group** [**mcast-vlan** *vlan-list*]	Show multicast VLAN and bound group address set of multicast VLAN copy.
5	Qtech#**show igmp vlan-copy-table** [**vlan** *vlan-id*] [**count**]	Show the multicast VLAN copy table.

6.7.5 Maintenance

Maintain the QSW-8200 series switch as below.

Command	Description
Qtech(config)#**clear igmp statistics** [*interface-type interface-number*]	Clear IGMP statistics.
Qtech(config)#**no igmp member** [*interface-type interface-number*]	Delete a specified multicast entry.

6.8 Configuration examples

6.8.1 Example for configuring IGMP Snooping

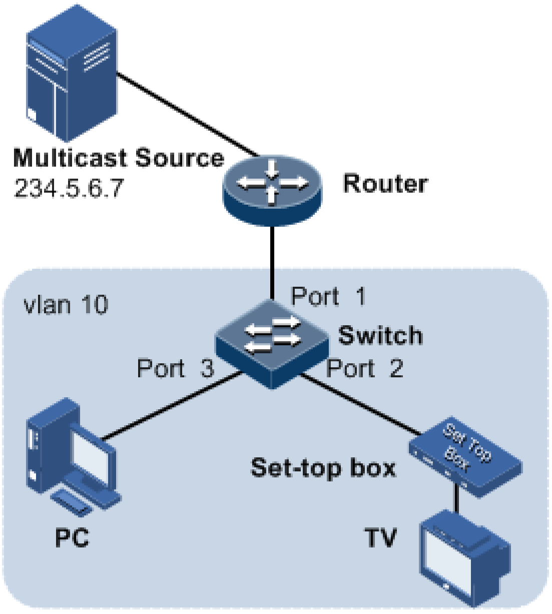
Networking requirements

As shown in Figure 6-7, Port 1 on the switch is connected with the multicast router; Port 2 and Port 3 connect users. All multicast users belong to the same VLAN 10; you need to configure IGMP Snooping on the switch to receive multicast data with the address 234.5.6.7.

Enable IGMP Proxy on the Switch to reduce communication between the PC and the multicast router, without implementing multicast.

When the PC and Set Top Box (STB) join the same multicast group, the Switch receives two copies of IGMP Report packets and then sends one copy to the multicast router. The IGMP Query packet sent by the multicast router will not forwarded to the downstream devices, but the Switch periodically send IGMP Query packets.

Figure 6-7 IGMP Snooping networking



Configuration steps

Step 1 Create a VLAN, and add interfaces to it.

```
Qtech#config
Qtech(config)#create vlan 10 active
Qtech(config)#interface port 1
Qtech(config-port)#switchport mode trunk
Qtech(config-port)#switchport trunk native vlan 10
Qtech(config-port)#exit
Qtech(config)#interface port 2
Qtech(config-port)#switchport access vlan 10
Qtech(config-port)#exit
Qtech(config)#interface port 3
Qtech(config-port)#switchport access vlan 10
Qtech(config-port)#exit
```

Step 2 Enable IGMP Snooping.

```
Qtech(config)#igmp snooping
Qtech(config)#igmp snooping vlan 10
```

Step 3 Configure IGMP Proxy.

```
Qtech(config)#igmp proxy
Qtech(config)#igmp proxy suppression
Qtech(config)#igmp proxy querier
Qtech(config)#igmp proxy source-ip 192.168.1.2
```

Checking results

Use the following command to show configurations of IGMP Snooping.

```
Qtech#show igmp snooping
  igmp snooping               :Enable
  igmp snooping active vlan      :10
  igmp router alert examine      :Disable
  igmp aging time(s)           :300
  igmp ring                   :--
```

Use the following command to show information about multicast group members of IGMP Snooping.

```
Qtech#show igmp snooping member vlan 10
Port           Vlan     GroupID        Live-time
-------------------------------------------------------
P1         10      234.5.6.7        270
```

Use the following command to show configurations of IGMP Proxy.

```
Qtech#show igmp proxy
Igmp Proxy Status              :Enable
Igmp Proxy Suppression Status   :Enable
Igmp Proxy Querier Status       :Enable
Igmp Proxy Source Ip            :192.168.1.2
Igmp Query Interval(s)           :60
Query Max Response Interval(s)  :10
Last Member Query Interval(s)   :1
Next IGMP General Query(s)     :10
```

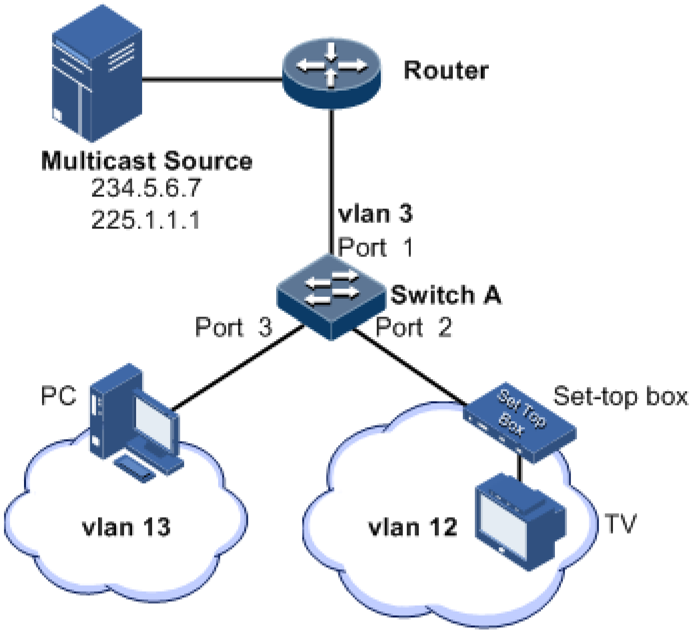
6.8.2 Example for configuring IGMP MVR

Networking requirements

As shown in Figure 6-8, Port 1 of the switch connects with the multicast router, and Port 2 and Port 3 connect with users in different VLANs to receive data from multicast 234.5.6.7 and 225.1.1.1.

Configure IGMP MVR on the Switch to designate VLAN 3 as a multicast VLAN, and then the multicast data can only be copied one time in the multicast VLAN instead of copying for each customer VLAN, thus saving bandwidth.

Figure 6-8 MVR networking



Configuration steps

Step 1 Create VLANs on Switch A and add interfaces to them.

```
Qtech(config)#config
Qtech(config)#creat vlan 3,12,13 active
Qtech(config)#interface port 1
Qtech(config-port)#switchport mode trunk
Qtech(config-port)#switchport trunk native vlan 3
Qtech(config-port)#switchport trunk untagged vlan 12,13
Qtech(config-port)#exit
Qtech(config)#interface port 2
Qtech(config-port)#switchport mode trunk
Qtech(config-port)#switchport trunk native vlan 12
Qtech(config-port)#switchport trunk untagged vlan 3
Qtech(config-port)#exit
Qtech(config)#interface port 3
Qtech(config-port)#switchport mode trunk
Qtech(config-port)#switchport trunk native vlan 13
Qtech(config-port)#switchport trunk untagged vlan 3
Qtech(config-port)#exit
```

Step 2 Configure IGMP MVR on Switch A.

```
Qtech(config)#igmp mvr
Qtech(config)#igmp mvr port 2,3
Qtech(config)#igmp mvr mcast-vlan 3 group 234.5.6.7
Qtech(config)#igmp mvr mcast-vlan 3 group 225.1.1.1
```

Checking results

Use the following command to show IGMP MVR configurations on Switch A.

```
Qtech#show igmp mvr
  igmp mvr running                    :Enable
  igmp mvr port                       :port-list 2-3
  igmp mvr multicast vlan(ref)        :3(2)
  igmp router alert examine           :Disable
  igmp aging time(s)                  :300
  igmp ring                           :--
```

Use the following command to show information about the multicast VLAN and group address.

```
Qtech#show igmp mvr vlan-group
mcast-vlan     start-group    end-group
-------------------------------------------
3              225.1.1.1      225.1.1.1
3              234.5.6.7      234.5.6.7
```

6.8.3 Example for applying IGMP filtering on interface

Networking requirements

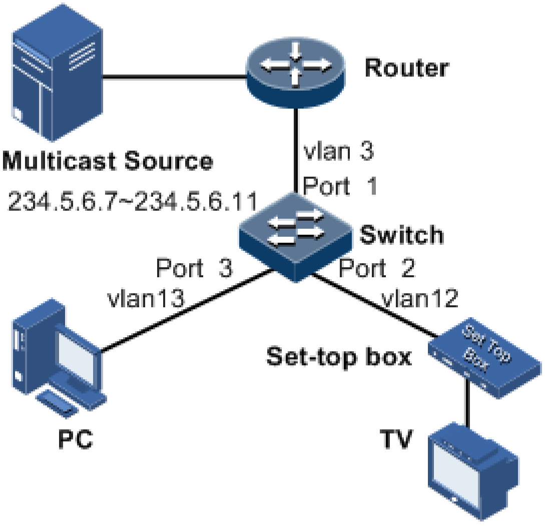
Enable IGMP filtering on the switch. Add filtering rules on the interface to filter multicast users.

As shown in Figure 6-9,

- Create an IGMP filtering rule Profile 1, set the action to pass for the multicast group ranging from 234.5.6.7 to 234.5.6.10.
- Apply filtering IGMP filtering rule Profile 1 on Port 2, allow the STB to join the 234.5.6.7 multicast group, forbid it to join the 234.5.6.11 multicast group.
- Apply no filtering rule on Port 3, and allow PCs to join the 234.5.6.11 multicast group.

Configure the maximum number of multicast groups on Port 2. After the STB is added to the 234.5.6.7 multicast group, add it to the 234.5.6.8 multicast group while it quits the 234.5.6.7 multicast group.

Figure 6-9 Applying IGMP filtering on interface



Configuration steps

Step 1 Create VLANs, and add interfaces into VLANs.

```
Qtech#config
Qtech(config)#creat vlan 3,12,13 active
Qtech(config)#interface port 1
Qtech(config-port)#switchport mode trunk
Qtech(config-port)#switchport trunk native vlan 3
Qtech(config-port)#switchport trunk untagged vlan 12,13
Qtech(config-port)#exit
Qtech(config)#interface port 2
Qtech(config-port)#switchport mode trunk
Qtech(config-port)#switchport trunk native vlan 12
Qtech(config-port)#switchport trunk untagged vlan 3
Qtech(config-port)#exit
Qtech(config)#interface port 3
Qtech(config-port)#switchport mode trunk
Qtech(config-port)#switchport trunk native vlan 13
Qtech(config-port)#switchport trunk untagged vlan 3
Qtech(config-port)#exit
```

Step 2 Enable IGMP MVR.

```
Qtech(config)#igmp mvr
Qtech(config)#igmp mvr port 2,3
Qtech(config)#igmp mvr mcast-vlan 3 group any
```

Step 3 Configure the IGMP filtering profile.

```
Qtech(config)#igmp filter profile 1
Qtech(config-igmp-profile)#permit
Qtech(config-igmp-profile)#range 1 234.5.6.7 234.5.6.10
Qtech(config-igmp-profile)#exit
```

Step 4 Configure the STB to apply the IGMP filter profile.

```
Qtech(config)#igmp filter
Qtech(config)#interface port 2
Qtech(config-port)#igmp filter profile 1
```

Step 5 Configure the maximum number of multicast groups on the STB interface.

```
Qtech(config-port)#igmp filter max-groups 1
Qtech(config-port)#igmp filter max-groups action replace
```

Checking results

Use the following command to show configurations of IGMP filtering on the interface.

```
Qtech#show igmp filter port 2
IGMP profile:  1
MaxGroup:      1
Currentgroup:  0
action:       replace
```

6.8.4 Example for applying multicast on ring network

Networking requirements

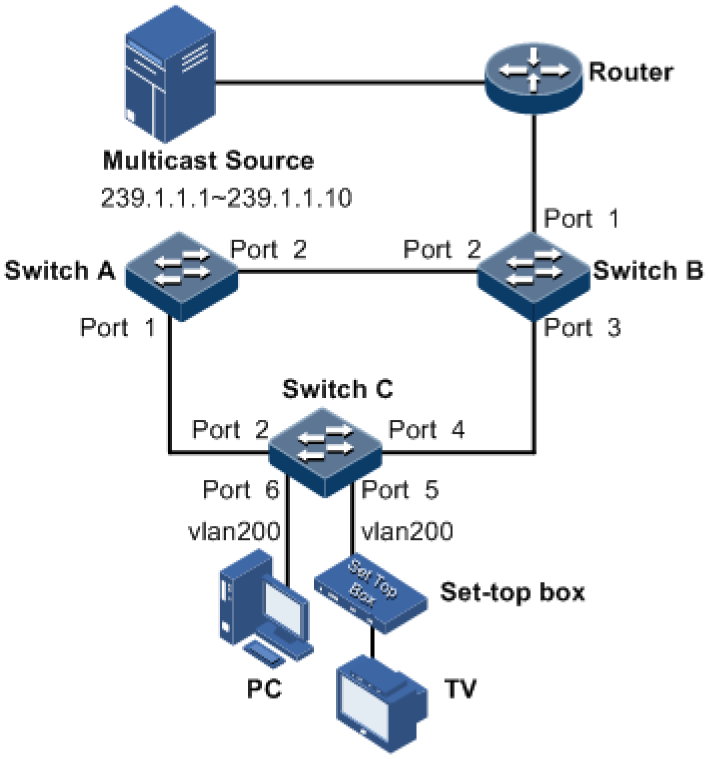
Configure IGMP ring forwarding on single Ethernet ring to make multicast service more stable and prevent multicast service from being disrupted by link failure.

As shown in Figure 6-10, Port 1 and Port 2 on Switch A, Port 2 and Port 3 on Switch B, Port 2 and Port 4 on Switch C form a physical ring. Multicast traffic is input from Port 1 on Switch B. The user demands multicast stream through Port 5 and Port 6 on Switch C. By doing this, whichever links fail in the Switch, it will not affect user's on-demand multicast stream.

When using single Ethernet ring to provide multicast services, you can adopt IGMP MVR or IGMP Snooping to receive the multicast stream.

The following example shows that STP provides ring network detection and IGMP Snooping provides multicast function.

Figure 6-10 Ring network multicast networking



Configuration steps

Step 1 Enable STP function, create a VLAN, and add interfaces into the VLAN.

Configure Switch A.

```
SwitchA#config
SwitchA(config)#spanning-tree enable
SwitchA(config)#spanning-tree mode stp
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport trunk native vlan 200
SwitchA(config)#exit
SwitchA(config-port)#interface port 2
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport trunk native vlan 200
```

Configure Switch B.

```
SwitchB#config
SwitchB(config)#spanning-tree enable
SwitchB(config)#spanning-tree mode stp
SwitchB(config)#interface port 2
SwitchB(config-port)switchport mode trunk
SwitchB(config-port)#switchport trunk native vlan 200
SwitchB(config-port)#exit
SwitchB(config)#interface port 3
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#switchport trunk native vlan 200
```

Configure Switch C.

```
SwitchC#config
SwitchC(config)#spanning-tree enable
SwitchC(config)#spanning-tree mode stp
SwitchC(config)#interface port 2
SwitchC(config-port)#switchport mode trunk
SwitchC(config-port)#switchport trunk native vlan 200
SwitchC(config-port)#exit
SwitchC(config)#interface port 4
SwitchC(config-port)#switchport mode trunk
SwitchC(config-port)#switchport trunk native vlan 200
```

Step 2 Enable IGMP Snooping and IGMP ring network forwarding on the interface.

Configure Switch A.

```
SwitchA(config)#igmp ring port-list 1,2
SwitchA(config)#igmp snooping
SwitchA(config)#igmp snooping vlan 200
```

Configure Switch B.

```
SwitchB(config)#igmp ring port-list 2,3
SwitchB(config)#igmp snooping
SwitchB(config)#igmp snooping vlan 200
```

Configure Switch C.

```
SwitchC(config)#igmp ring port-list 2,4
SwitchC(config)#igmp snooping
SwitchC(config)#igmp snooping vlan 200
```

Checking results

Disconnect any link in the ring, and check whether the multicast flow can be received normally.

7 Security

This chapter describes basic principles and configurations of security, and provides related configuration examples, including the following sections:

- Port security MAC
- ACL
- Dynamic ARP inspection
- RADIUS
- TACACS+
- 802.1x
- PPPoE+
- Storm control

7.1 Port security MAC

7.1.1 Introduction

Port security MAC is used for the Switch on the edge of the network user side, which can ensure security of access data on an interface, control the ingress packets according to source MAC address.

You can start port security MAC to limit and distinguish those users which can access the network through the secure port. Only the secure MAC address can access the network, unsecure MAC address will be processed as configured violation mode for interface access.

Classification secure MAC address

The QSW-8200 series switch supports the secure MAC address, which is divided into the following three types:

- Static secure MAC address

The static secure MAC address is configured by users on the secure port manually. This MAC address will take effect when the secure MAC address is enabled. This type of secure MAC addresses is not aged and supports loading configurations.

- Dynamic secure MAC address

The dynamic secure MAC address is learnt by the QSW-8200 series switch. You can set the learnt MAC address to secure MAC address in the range of the maximum number of learning MAC address. This type of secure MAC addresses is aged and does not support loading configurations.

The dynamic secure MAC address can be converted to the sticky secure MAC address as required, so as not to be aged and support loading configurations.

- Sticky secure MAC address

The sticky secure MAC address is generated from the manual configuration of users in secure interface or converted from dynamic secure MAC address. Different from static secure MAC address, sticky secure MAC address needs to be used in conjunction with sticky learning:

  - When sticky learning is enabled, sticky secure MAC address will take effect and this address will not be aged and support loading configurations.
  - When sticky learning is disabled, sticky secure MAC address will lose effectiveness and be saved only in the system.

Note

- When sticky learning is enabled, all the dynamic secure MAC addresses learnt on the interface will be converted to sticky secure MAC addresses.
- When sticky learning is disabled, all the sticky secure MAC addresses on the interface will be converted to dynamic secure MAC addresses.

Processing mode for secure MAC violations

When the number of secure MAC addresses has already reached the maximum number, the entry of strange source MAC address packets will be regarded as violation operation. For the illegal user access, there are different processing modes to configure the Switch according to secure MAC violation policy:

- Protect mode: for illegal users, the secure interface discards the user's packets directly.
- Restrict mode: for illegal users, the secure interface discards user's packets, the console prints Syslog information and sends alarm to the network management system.
- Shutdown mode: for illegal users, the secure interface discards user's packets, and the console prints Syslog information, sends alarm to the network management system, and then shuts down the secure interface.

Caution

When the MAC address is in drift, that is, the secure interface A receives one user access corresponding a secure MAC address on secure interface B, secure interface A will process it as a security violation.

7.1.2 Preparing for configurations

Scenario

To ensure security of data accessing an interface, you can control the input packets according to source MAC address. Through secure MAC address, you can configure to permit specified users to access the interface, and permit a specified numbers of users to access from this interface only. However, when the number of access users exceeds the limit, the access interface will take operation according to secure MAC address violation policies.

Prerequisite

N/A

7.1.3 Default configurations of port security MAC

Default configurations of port security MAC are as below.

Function	Default value
Port security MAC status	Disable
Dynamic secure MAC aging time	300min
Dynamic secure MAC sticky learning status	Disable
Port security MAC sending Trap status	Disable
Port security MAC violation processing mode	Protection mode
Maximum number of port security MAC addresses	1024

7.1.4 Configuring basic functions of port security MAC

Caution

- We do not recommend enabling port security MAC on LAG member interfaces.
- We do not recommend using MAC address management function to configure static MAC addresses when port security MAC is enabled.
- Port security MAC and Dot1x are mutually exclusive, which cannot be configured concurrently.
- Port security MAC and MAC address limit based on interface and interface VLAN are mutually exclusive, which cannot be configured concurrently.

Configure basic functions of port security MAC for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**switchport port-security**	Enable port security MAC.
4	Qtech(config-port)#**switchport port-security maximum** *maximum*	(Optional) configure the maximum number of secure MAC addresses.
5	Qtech(config-port)#**switchport port-security violation** { **protect** | **restrict** | **shutdown** }	(Optional) configure port security MAC violation mode.

Step	Command	Description
6	Qtech(config-port)#**no port-security shutdown**	(Optional) re-enable the interface which is shut down due to violating port security MAC.

Note

- When port security MAC violation policy is in Shutdown mode, you can use this command to re-enable this interface which is shut down due to violating secure MAC address.
- When the interface is Up, the configured port security MAC violation mode will continue to be valid.

7.1.5 Configuring static secure MAC address

Configure the static secure MAC address for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**switchport port-security mac-address** *mac-address* **vlan** *vlan-id*	Configure the static secure MAC address.
4	Qtech(config-port)#**switchport port-security**	Enable port security MAC.

7.1.6 Configuring dynamic secure MAC address

Configure the dynamic secure MAC address for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**port-security aging-time** *period*	(Optional) configure the aging time of secure MAC addresses.
3	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
4	Qtech(config-port)#**switchport port-security**	Enable dynamic secure MAC address learning.
5	Qtech(config-port)#**switchport port-security trap enable**	(Optional) enable port security MAC to send Trap.

Note

Use the **switchport port-security** command to enable port security MAC and dynamic secure MAC address learning concurrently.

7.1.7 Configuring sticky secure MAC address

Configure the sticky secure MAC address for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**switchport port-security**	Enable port security MAC.
4	Qtech(config-port)#**switchport port-security mac-address sticky** *mac-address* **vlan** *vlan-id*	(Optional) configure the port sticky secure MAC address manually.
5	Qtech(config-port)#**switchport port-security mac-address sticky**	Enable sticky secure MAC address learning. Note After enabling sticky secure MAC address learning, the dynamic secure MAC address will be converted to the sticky secure MAC address; the manually configured sticky secure MAC address will take effect.

7.1.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show port-security** [**port-list** *port-list*]	Show configurations of secure MAC addresses on the interface.
2	Qtech#**show port-security mac-address** [**port-list** *port-list*]	Show configurations of secure MAC address and learning status.

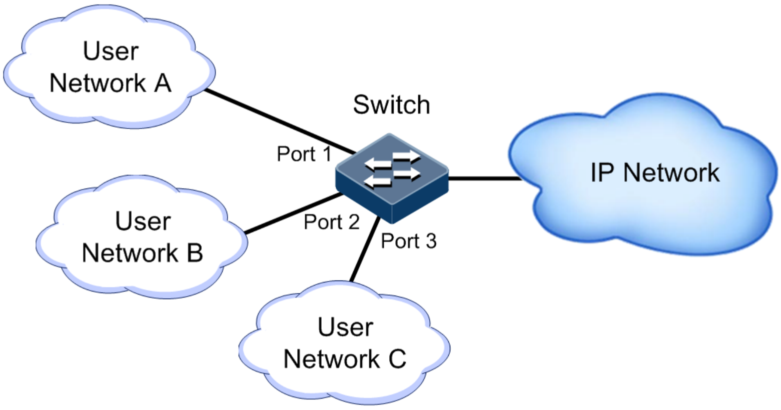
7.1.9 Example for configuring port security MAC

Networking requirements

As shown in Figure 7-1, the Switch connects 3 user networks. To ensure security of data accessing on the interface, configure the Switch as below.

- The port 1 permits up to 3 users to access the network. One of specified user MAC addresses is 0000.0000.0001. The other two users are in dynamic learning mode. The network management system can receive Trap information once the user learns a MAC address. The violation mode is Protect mode and the aging time of the two learning user MAC addresses is 10min.
- The port 2 permits up to 2 users to access the network. MAC addresses of the 2 users are determined through learning; once they are learnt, they will not be aged. The violation mode is Restrict mode.
- The port 3 permits up to 1 user to access the network. The specified user MAC address is 0000.0000.0002. Whether MAC addresses are aged can be controlled. The violation mode is Shutdown mode.

Figure 7-1 Port security MAC networking



Configuration steps

Step 1 Configure secure MAC address on port 1.

```
Qtech#config
Qtech(config)#interface port 1
Qtech(config-port)#switchport port-security
Qtech(config-port)#switchport port-security maximum 3
Qtech(config-port)#switchport port-security mac-address 0000.0000.0001
vlan 1
Qtech(config-port)#switchport port-security violation protect
Qtech(config-port)#switchport port-security trap enable
Qtech(config-port)#exit
Qtech(config)#port-security aging-time 10
```

Step 2 Configure secure MAC address on port 2.

```
Qtech(config)#interface port 2
Qtech(config-port)#switchport port-security
Qtech(config-port)#switchport port-security maximum 2
Qtech(config-port)#switchport port-security mac-address sticky
Qtech(config-port)#switchport port-security violation restrict
Qtech(config-port)#exit
```

Step 3 Configure secure MAC address for port 3.

```
Qtech(config)#interface port 3
Qtech(config-port)#switchport port-security
Qtech(config-port)#switchport port-security maximum 1
Qtech(config-port)#switchport port-security mac-address sticky
0000.0000.0002 vlan 1
Qtech(config-port)#switchport port-security mac-address sticky
Qtech(config-port)#switchport port-security violation shutdown
```

Checking results

Use the **show port-security** [**port-list** *port-list*] command to show configurations of port security MAC.

```
Qtech#show port-security port-list 1-3
Port security aging time:10 (mins)
port status  Max-Num  Cur-Num  His-Num   vio-Count vio-action Dynamic-Trap
--------------------------------------------------------------------------
P1    Enable    3        1       0           0       protect      Enable
P2    Enable    2        0       0           0       restrict     Disable
P3    Enable    1        1       0           0       shutdown     Disable
```

Use the **show port-security mac-address** command to show configurations and learning of secure MAC address.

```
Qtech#show port-security mac-address
VLAN  Security-MAC-Address  Flag    Port  Age(min)
-------------------------------------------------
2     0000.0000.0001       static    P1    --
2     0000.0000.0002       sticky    P3    --
```

7.2 ACL

7.2.1 Introduction

Access Control List (ACL) is a set of ordered rules, which can control the QSW-8200 series switch to receive or discard some data packets, thus prevent illegal packets from impacting network performance.

ACL is composed of **permit** | **deny** sentences. The rules are described by the source MAC address, destination MAC address, source IP address, destination IP address, and port ID of data packets. The QSW-8200 series switch determines whether to receive or discard packets according to these rules.

7.2.2 Preparing for configurations

Scenario

ACL can help a network device to recognize objects to be filtered. The device recognizes special objects and then permits/denies packets to pass according to the configured policy.

ACL includes the below types:

- IP ACL: make classification rule according to source or destination address taken by packets IP head, port ID used by TCP or UDP, etc. attributes.
- MAC ACL: make classification rule according to source MAC address, destination MAC address, Layer 2 protocol type taken by packet Layer 2 frame head, etc. attributes.
- MAP ACL: MAP ACL can define more protocols and more detailed protocol fields than IP ACL and MAC ACL, also can match any bytes from 22 to 63 of Layer 2 data frame according to user's definition (the offset is starting from 0).

There are 4 kinds of ACL applications according to difference of application environment: based on the whole device, based on interface, based on flow from the ingress interface to the egress interface, and based on VLAN.

Prerequisite

N/A

7.2.3 Default configurations of ACL

Default configurations of ACL are as below.

Function	Default value
Device filtering status	Disable
Filter effectiveness status	Allowed to take effect
MAC address matching rules	Mismatch
CoS value matching rules	Mismatch
Ethernet frame type matching rules	Mismatch
ARP protocol type matching rules	Mismatch

Function	Default value
ARP packet and MAC/IP address matching rules	Mismatch
IP packet matching rules	Mismatch
TCP packet matching rules	Mismatch
UDP packet matching rules	Mismatch
IGMP packet message type matching rules	Mismatch
IPv6 packet matching rules	Mismatch
VLAN ID matching rules	Mismatch

7.2.4 Configuring IP ACL

Configure IP ACL for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**ip-access-list** *acl-number* { **deny** | **permit** } { *protocol-id* | **icmp** | **igmp** | **ip** } { *source-ip-address ip-mask* | **any** } { *destination-ip-address ip-mask* | **any** }	Configure IP ACL.
	Qtech(config)#**ip-access-list** *acl-number* { **deny** | **permit** } { **tcp** | **udp** } { *source-ip-address ip-mask* | **any** } [*source-protocol-port*] { *destination-ip-address ip-mask* | **any** } [*destination-protocol-port*]	

7.2.5 Configuring IPv6 ACL

Configure IPv6 ACL for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**ipv6-access-list** *acl-number* { **deny** | **permit** } { *next-header-value* | **icmpv6** | **ipv6** } [**traffic-class** *class-id*] [**flow-label** *label-id*] { *source-ipv6-address/mask* | **any** } { *destination-ipv6-address/mask* | **any** }	Configure binding protocol type as ICMPv6, IPv6 or input protocol type ID IPv6 ACL.

Step	Command	Description
3	Qtech(config)#**ipv6-access-list** *acl-number* { **deny** | **permit** } { **tcp** | **udp** } [**traffic-class** *class-id*] [**flow-label** *label-id*] { *source-ipv6-address/mask* | **any** } [*source-protocol-port*] { *destination-ipv6-address/mask* | **any** } [*destination-protocol-port*]	Configure binding protocol type as TCP or UDP IPv6 ACL.

7.2.6 Configuring MAC ACL

Configure MAC ACL for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**mac-access-list** *acl-number* { **deny** | **permit** } [*protocol-id* | **arp** | **ip** | **rarp** | **any**] { *source-mac-address mask* | **any**} { *destination-mac-address mask* | **any** }	Configure MAC ACL.

7.2.7 Configuring MAP ACL

Configure MAP ACL for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**access-list-map** *acl-number* { **deny** | **permit** }	Create a MAP ACL, and enter ACLMAP configuration mode.
3	Qtech(config-aclmap)#**match mac** { **destination** | **source** } *mac-address mask*	(Optional) define matching rules for the source or destination MAC address. By default, the MAC address is not matched.
4	Qtech(config-aclmap)#**match cos** *cos-value*	(Optional) define matching rules for Cos value. By default, CoS is configured.
5	Qtech(config-aclmap)#**match ethertype** *ethertype* [*ethertype-mask*]	(Optional) define matching rules for Ethernet frame type. By default, Ethernet frame type is not matched. Both *ethertype* and *ethertype-mask* are hex-decimal digitals in format of HHHH.

Step	Command	Description
6	Qtech(config-aclmap)#**match** { **arp** | **eapol** | **flowcontrol** | **ip** | **ipv6** | **loopback** | **mpls** | **mpls-mcast** | **pppoe** | **pppoedisc** | **slowprotocol** | **x25** | **x75** }	(Optional) define matching rules for upper layer protocol type carried by laryer-2 packets head.
7	Qtech(config-aclmap)#**match arp opcode** { **reply** | **request** }	(Optional) define matching rules for ARP protocol type (reply packet/request packet). By default, ARP type is not matched.
8	Qtech(config-aclmap)#**match arp** { **sender-mac** | **target-mac** } *mac-address*	(Optional) define matching rules for the MAC address of ARP packets. By default, the MAC address of ARP packets is not matched.
9	Qtech(config-aclmap)#**match arp** { **sender-ip** | **target-ip** } *ip-address* [*ip-mask*]	(Optional) define matching rules for the IP address of ARP packets. By default, the IP address of ARP packets is not matched.
10	Qtech(config-aclmap)#**match ip** { **destination-address** | **source-address** } *ip-address* [*ip-mask*]	(Optional) define matching rules for the source or destination IP address. By default, the IP address is not matched.
11	Qtech(config-aclmap)#**match ip precedence** { precedence-value | **critical** | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine** }	(Optional) define matching rules for priority of IP packets. By default, the priority of IP packets is not matched.
12	Qtech(config-aclmap)#**match ip tos** { tos-value | **max-reliability** | **max-throughput** | **min-delay** | **min-monetary-cost** | **normal** }	(Optional) define matching rules for ToS value of IP packet priority. By default, the ToS value of priority of IP packets is not matched.
13	Qtech(config-aclmap)#**match ip dscp** { dscp-value | **af11** | **af12** | **af13** | **af21** | **af22** | **af23** | **af31** | **af32** | **af33** | **af41** | **af42** | **af43** | **cs1** | **cs2** | **cs3** | **cs4** | **cs5** | **cs6** | **cs7** | **default** | **ef** }	(Optional) define matching rules for DSCP value of IP packet. By default, the DSCP value of IP packets is not matched.
14	Qtech(config-aclmap)#**match ip protocol** { *protocol-id* | **ahp** | **esp** | **gre** | **icmp** | **igmp** | **igrp** | **ipinip** | **ospf** | **pcp** | **pim** | **tcp** | **udp** }	(Optional) define matching rules for protocol value of IP packet. By default, the protocol value of IP packets is not matched.

Step	Command	Description
15	Qtech(config-aclmap)#**match ip tcp** { **destination-port** | **source-port** } { port-id | **bgp** | **domain** | **echo** | **exec** | **finger** | **ftp** | **ftp-data** | **gopher** | **hostname** | **ident** | **irc** | **klogin** | **kshell** | **login** | **lpd** | **nntp** | **pim-auto-rp** | **pop2** | **pop3** | **smtp** | **sunrpc** | **syslog** | **tacacs** | **talk** | **telnet** | **time** | **uucp** | **whois** | **www** }	(Optional) define matching rules for port ID of TCP packet. By default, the port ID of TCP packets is not matched.
16	Qtech(config-aclmap)#**match ip tcp** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** }	(Optional) define matching rules for TCP protocol tag. By default, the TCP protocol tag is not matched.
17	Qtech(config-aclmap)#**match ip udp** { **destination-port** | **source-port** } { port-id | **biff** | **bootpc** | **bootps** | **domain** | **echo** | **mobile-ip** | **netbios-dgm** | **netbios-ns** | **netbios-ss** | **ntp** | **pim-auto-rp** | **rip** | **snmp** | **snmptrap** | **sunrpc** | **syslog** | **tacacs** | **talk** | **tftp** | **time** | **who** }	(Optional) Define matching rules for port ID of UDP packet. By default, the port ID of UDP packets is not matched.
18	Qtech(config-aclmap)#**match ip icmp** *icmp-type-id* [*icmp-code*]	(Optional) define matching rules for message type of ICMP packets. By default, the message type of ICMP packets is not matched.
19	Qtech(config-aclmap)#**match ip igmp** { *igmp-type-id* | **dvmrp** | **leave-v2** | **pim-v1** | **query** | **report-v1** | **report-v2** | **report-v3** }	(Optional) define matching rules for message type of IGMP packets. By default, the match message type of IGMP packets is not matched.
20	Qtech(config-aclmap)#**match ipv6**	(Optional) define matching rule for IPv6 packet. By default, IPv6 packets are not matched.
21	Qtech(config-aclmap)#**match** { **svlan** | **cvlan** } *vlan-id*	(Optional) define matching rules for VLAN ID. By default, VLAN ID is not matched.

Step	Command	Description
22	`Qtech(config-aclmap)#match user-define rule-string rule-mask offset`	(Optional) configure matching rules for user-defined field, that is, two parameters of rule mask and offset take any byte from 22 to 63 of data frame (the offset is starting from 0), then comparing with user-defined rule to filter out matched data frame for processing. For example, if you wish to filter all TCP packets, you can defines the rule as 06, rule mask as EF, offset as 27; the rule mask and offset value work together to filter out content of TCP protocol ID field, then compare with rule and match with all TCP packets. **Note** A rule must be an even number of hex digital. The offset includes field 802.1q VLAN Tag regardless that the QSW-8200 series switch receives Untag packets.

7.2.8 Applying ACL

Configure ACL for the QSW-8200 series switch as below.

Note

ACL cannot take effect until it is added into a filter. Multiple ACL matching rules can be added into a filter to form multiple filtering rules. When you configure the filter, the order to add ACL matching rules decides priority of the rule. The later a rule is added, the higher the priority is. If the multiple rules conflict in matching calculation, take the higher priority rule as standard. Pay attention to the order of rules when setting the commands to filter packets correctly.

- ACL application on the whole device

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#filter { access-list-map | ip-access-list | ipv6-access-list | mac-access-list } { all | acl-list } [ statistics ]`	Configure filter for the whole device. If the **statistics** parameter is configured, the system will take statistics according to filtering rule.
	`Qtech(config)#filter { access-list-map | ip-access-list | ipv6-access-list | mac-access-list } { all | acl-list } valid`	(Optional) enable the filter on the whole device.

Step	Command	Description
4	Qtech(config)#**filter enable**	Enable the filter and rules. Enabling the filter can both active the filtering rules and make the filtering rules set later take effect. By default, the filter is disabled. Use the **filter disable** command to disable the filter.

- ACL application based on interface

Step	Command	Description
1	Qtech#**config**	Enable the filter and rules. Enabling the filter can both active the filtering rules and make the filtering rules set later take effect. By default, the filter is not enabled. Use the **filter disable** command to disable the filter.
2	Qtech(config)#**filter { access-list-map | ip-access-list | ipv6-access-list | mac-access-list } { all |** *acl-list* **} { ingress | egress } port-list** *port-list* **[statistics]**	Configure filter on interface. If the **statistics** parameter is configured, the system will take statistics according to filtering rule.
3	Qtech(config)#**filter { access-list-map | ip-access-list | ipv6-access-list | mac-access-list } { all |** *acl-list* **} { ingress | egress } port-list** *port-list* **valid**	(Optional) enable interface filter.
4	Qtech(config)#**filter enable**	Enable the filter and rules. Enabling the filter can both active the filtering rules and make the filtering rules set later take effect. By default, the filter is not enabled. Use the **filter disable** command to disable the filter.

- ACL application based on flow from the ingress interface to the egress interface

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.

Step	Command	Description
2	Qtech(config)#**filter** { **access-list-map** | **ip-access-list** | **ipv6-access-list** | **mac-access-list** } { **all** | *acl-list* } **from** *inport-id* **to** *outport-id* [**statistics**]	Configure flow filter from ingress interface to the egress interface. If the **statistics** parameter is configured, the system will take statistics according to filtering rules.
3	Qtech(config)#**filter** { **access-list-map** | **ip-access-list** | **ipv6-access-list** | **mac-access-list** } { **all** | *acl-list* } **from** *inport-id* **to** *outport-id* **valid**	(Optional) enable flow filter from the ingress interface to the egress interface.
4	Qtech(config)#**filter enable**	Enable the filter and rules. Enabling the filter can both active the filtering rules and make the filtering rules set later take effect. By default, the filter is not enabled. Use the **filter disable** command to disable the filter.

- ACL application based on VLAN

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**filter** { **access-list-map** | **ip-access-list** | **ipv6-access-list** | **mac-access-list** } { **all** | *acl-list* } **vlan** *vlan-id* [**double-tagging inner**] [**statistics**]	Configure VLAN filter. If the **statistics** parameter is configured, the system will take statistics according to filtering rules.
3	Qtech(config)#**filter** { **access-list-map** | **ip-access-list** | **ipv6-access-list** | **mac-access-list** } { **all** | *acl-list* } **vlan** *vlan-id* [**double-tagging inner**] **valid**	(Optional) enable the VLAN filter.
4	Qtech(config)#**filter enable**	Enable the filter and rules. Enabling the filter can both active the filtering rules and make the filtering rules set later take effect. By default, the filter is not enabled. Use the **filter disable** command to disable the filter.

Note

The created filtering rules permit the filter function to take effect. At this time:

- If the global filter is enabled, the filter function in corresponding filter list will take effect instantly.

- If the global filter is disabled, the filtering rules in filter ACL list will not take effect immediately, and the permit label is only for software record. After the global filter is enabled, the filter permit/deny function will be written to hardware.
- To permit the filter function to take effect cannot change the priority order of each filter; the priority is still subject to the filter priority when it is created.

The created filtering rules deny the filter function to take effect. At this time:

- If the global filter is enabled, the filtering rules will become invalid instantly; the hardware enabled label corresponding to filtering rules will be set to disable status immediately.
- If the global filter is disabled, the filtering rules are only for software record. When the global filter function is enabled, the hardware enabled label corresponding to filtering rules will be written to disable status.

7.2.9 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show ip-access-list** [*acl-list*]	Show configurations of IP ACL.
2	Qtech(config)#**show ipv6-access-list** [*acl-list*]	Show configurations of IPv6 ACL.
3	Qtech(config)#**show mac-access-list** [*acl-list*]	Show configurations of MAC ACL.
4	Qtech(config)#**show access-list-map** [*acl-number*]	Show configurations of MAP ACL.
5	Qtech(config)#**show filter**	Show filter configurations.
6	Qtech(config)#**show filter** { **access-list-map** | **ip-access-list** | **ipv6-access-list** | **mac-access-list** } { **all** | *acl-list* }	Show filter configurations for the whole device.
7	Qtech(config)#**show filter** { **access-list-map** | **ip-access-list** | **ipv6-access-list** | **mac-access-list** } { **all** | *acl-list* } { **ingress** | **egress** } **port-list** *port-list*	Show configurations of interface filter.
8	Qtech(config)#**show filter** { **access-list-map** | **ip-access-list** | **ipv6-access-list** | **mac-access-list** }{ **all** | *acl-list* } **from port** *inport-id* **to port** *outport-id*	Show the flow filter configurations from the ingress interface to the egress interface.
9	Qtech(config)#**show filter**{ **access-list-map** | **ip-access-list** | **ipv6-access-list** | **mac-access-list** } { **all** | *acl-list* } **vlan** *vlan-id* [**double-tagging inner**]	Show VLAN filter configurations.

7.2.10 Maintenance

Maintain the QSW-8200 series switch as below.

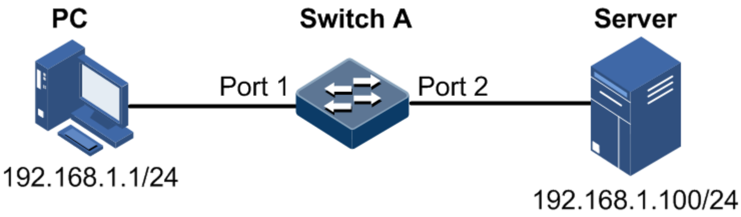
Command	Description
Qtech(config)#**clear filter statistics**	Clear filter statistics.
Qtech(config)#**clear filter** { **access-list-map** | **ip-access-list** | **ipv6-access-list** | **mac-access-list** } { **all** | *acl-list* } **statistics**	Clear statistics of filters on the whole device.
Qtech(config)#**clear filter** { **access-list-map** | **ip-access-list** | **ipv6-access-list** | **mac-access-list** } { **all** | *acl-list* } { **ingress** | **egress** } **port-list** *port-list* **statistics**	Clear statistics of filters on the interface.
Qtech(config)#**clear filter** { **access-list-map** | **ip-access-list** | **ipv6-access-list** | **mac-access-list** } { **all** | *acl-list* } **from port** *inport-id* **to port** *outport-id* **statistics**	Clear statistics of filters on the flow from form the ingress interface to the egress interface.
Qtech(config)#**clear filter** { **access-list-map** | **ip-access-list** | **ipv6-access-list** | **mac-access-list** } { **all** | *acl-list* } **vlan** *vlan-id* [**double-tagging inner**] **statistics**	Clear VLAN filter statistics.

7.2.11 Example for configuring ACL

Networking requirements

As shown in Figure 7-2, to prevent users from accessing the server, configure ACL to deny the PC with the IP address 192.168.1.1 of accessing the server with the IP address 192.168.1.100 on Switch A.

Figure 7-2 ACL networking



Configuration steps

Step 1 Configure IP ACL.

```
Qtech#config
Qtech(config)#ip-access-list 1 permit ip any any
Qtech(config)#ip-access-list 2 deny ip 192.168.1.1 255.255.255.255
192.168.1.100 255.255.255.255
```

Step 2 Apply ACL to port 1 on Switch A.

```
Qtech(config)#filter ip-access-list 1-2 ingress port-list 1
Qtech(config)#filter enable
```

Checking results

Use the **show ip-access-list** command to show configurations of IP ACL.

```
Qtech#show ip-access-list
Src Ip: Source Ip Address
Dest Ip: Destination Ip Address
List  Access   Protocol Ref. Src Ip:Port         Dest Ip:Port
------------------------------------------------------------------
1    permit   IP      1    0.0.0.0:0          0.0.0.0:0
2    deny     IP      1    192.168.1.0:0       192.168.1.100:0
```

Use the **show filter** command to show filter configurations.

```
Qtech#show filter
Rule filter: Enable
Filter list(Larger order number, Higher priority):
ACL-Index  IPort   EPort   VLAN VLANType Hardware StatHw   Pkts
-------------------------------------------------------------------
IP   1      P1   --       --  --      Yes     No      --
IP   2      P1   --       --  --      Yes     No      --
```

7.3 Dynamic ARP inspection

7.3.1 Introduction

Dynamic ARP inspection is used for ARP protection of unsecure interface and prevents from responding ARP packets which do not meet the requirements, thus preventing ARP spoofing attack on the network.

Principle of dynamic ARP inspection

There are 2 modes for dynamic ARP inspection:

- Static binding mode: set the binding manually.
- Dynamic binding mode: in cooperation with DHCP Snooping to generate dynamic binding. When DHCP Snooping entry is changed, the dynamic ARP inspection will also update dynamic binding entry synchronously.

The ARP inspection table, which is used for preventing ARP attacks, consists of DHCP Snooping entries and statically configured ARP inspection rules, including IP address, MAC address, and VLAN binding information. In addition, the ARP inspection table associates this information with specific interfaces. The dynamic ARP inspection binding table supports the combination of following entries:

- Interface+IP
- Interface+IP+MAC
- Interface+IP+VLAN
- Interface+IP+MAC+VLAN

Dynamic ARP inspection interfaces are divided into the following two types according to trust status:

- Trusted interface: the interface will stop ARP inspection, which conducts no ARP protection on the interface. All ARP packets are allowed to pass.
- Untrusted interface: the interface takes ARP protection. Only ARP packets that match the binding table rules are allowed to pass. Otherwise, they are discarded.

Figure 7-3 Principle of dynamic ARP inspection

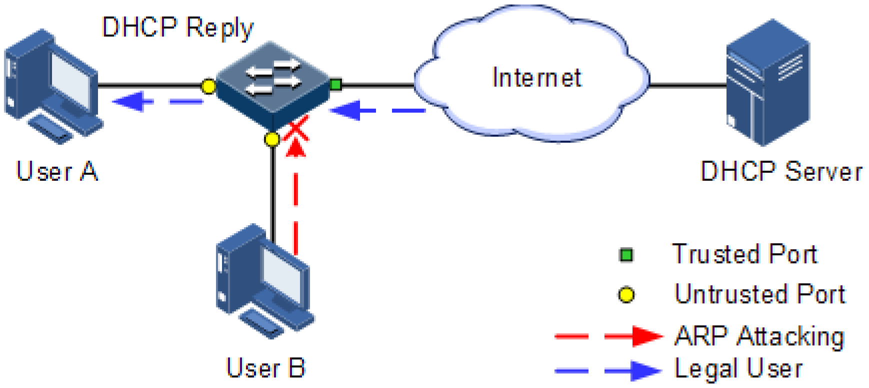


Figure 7-3 shows the principle of dynamic ARP inspection. When the QSW-8200 series switch receives an ARP packet, it compares the source IP address, source MAC address, interface ID, and VLAN information about the ARP packet with the DHCP Snooping entry information. If matched, it indicates that it is a legal user and the ARP packet is permitted to pass. Otherwise, it is an ARP attack and the ARP packet is discarded.

Rate limiting on ARP packets on interface

Dynamic ARP inspection also provides rate limiting on ARP packets to prevent unauthorized users from attacking the QSW-8200 series switch by sending a large number of ARP packets to the QSW-8200 series switch.

- When the number of ARP packets received by an interface every second exceeds the threshold, the system will regard that the interface receives an ARP attack, and then discard all received ARP packets to avoid the attack.
- The system provides auto-recovery and supports configuring the recovery time. The interfaces, where the number of received ARP packets is greater than the threshold, will recover to normal Rx/Tx status automatically after the recovery time expires.

Protection VLAN

Dynamic ARP inspection can also protect the specified VLAN. After the protection VLAN is configured, the ARP packets in specified VLAN on an untrusted interface will be protected.

Only the ARP packets, which meet binding table rules, are permitted to pass. Other packets are discarded.

7.3.2 Preparing for configurations

Scenario

Dynamic ARP inspection is used to prevent the common ARP spoofing attacks on the network, which isolates the ARP packets with unsafe sources. Trust status of an interface depends on whether it trusts ARP packets. However, the binding table decides whether the ARP packets meet requirement.

Prerequisite

Enable DHCP Snooping if there is a DHCP user.

7.3.3 Default configurations of dynamic ARP inspection

Default configurations of dynamic ARP inspection are as below.

Function	Default value
Dynamic ARP inspection interface trust status	Untrusted
Dynamic ARP inspection static binding	Disable
Dynamic ARP inspection static binding table	N/A
Dynamic ARP inspection protection VLAN	All VLANs
Interface rate limiting status for ARP packets	Disable
Interface rate limiting on ARP packets	100 pps
Auto-recovery rate limiting on ARP packets	Disable
Auto-recovery time for rate limiting on ARP packets	30s

7.3.4 Configuring trusted interfaces of dynamic ARP inspection

Configure trusted interfaces of dynamic ARP inspection for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Qtech(config-port)#`**`ip arp-inspection trust`**	Set the interface to a trusted interface. Use the **no ip arp-inspection trust** command to set the interface to an untrusted interface, that is, the interface does not trust the ARP packet.

7.3.5 Configuring static binding of dynamic ARP inspection

Configure static binding of dynamic ARP inspection for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**ip arp-inspection static-config**	Enable global static ARP binding.
3	Qtech(config)#**ip arp-inspection binding** *ip-address* [*mac-address*] [**vlan** *vlan-id*] **port** *port-id*	Configure the static binding.

7.3.6 Configuring dynamic binding of dynamic ARP inspection

Caution

Before enabling dynamic binding of dynamic ARP inspection, use the **ip dhcp snooping** command to enable DHCP Snooping.

Configure dynamic binding of dynamic ARP inspection for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**ip arp-inspection dhcp-snooping**	Enable global dynamic ARP binding.

7.3.7 Configuring protection VLAN of dynamic ARP inspection

Configure protection VLAN of dynamic ARP inspection for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**ip arp-inspection dhcp-snooping**	Enable global dynamic ARP binding.
3	Qtech(config)#**ip arp-inspection vlan** *vlan-list*	Configure the protection VLAN of dynamic ARP inspection

7.3.8 Configuring rate limiting on ARP packets on interface

Configure rate limiting on ARP packets on the interface for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#interface port port-id`	Enter physical layer interface configuration mode.
3	`Qtech(config-port)#ip arp-rate-limit enable`	Enable interface ARP packet rate limiting.
4	`Qtech(config-port)#ip arp-rate-limit rate rate-value`	Configure rate limiting on ARP packets on the interface.

7.3.9 Configuring auto-recovery time for rate limiting on ARP packets

Configure the auto-recovery time for rate limiting on ARP packets for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#ip arp-rate-limit recover enable`	Enable auto-recovery for rate limiting on ARP packets.
3	`Qtech(config)#ip arp-rate-limit recover time seconds`	Configure the auto-recovery time for rate limiting on ARP packets. By default, it is 30s.

7.3.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Qtech#show ip arp-inspection`	Show configurations of dynamic ARP inspection.
2	`Qtech#show ip arp-inspection binding [ port port-id ]`	Show information about the dynamic ARP inspection binding table.
3	`Qtech#show ip arp-rate-limit`	Show configurations of rate limiting on ARP packets.

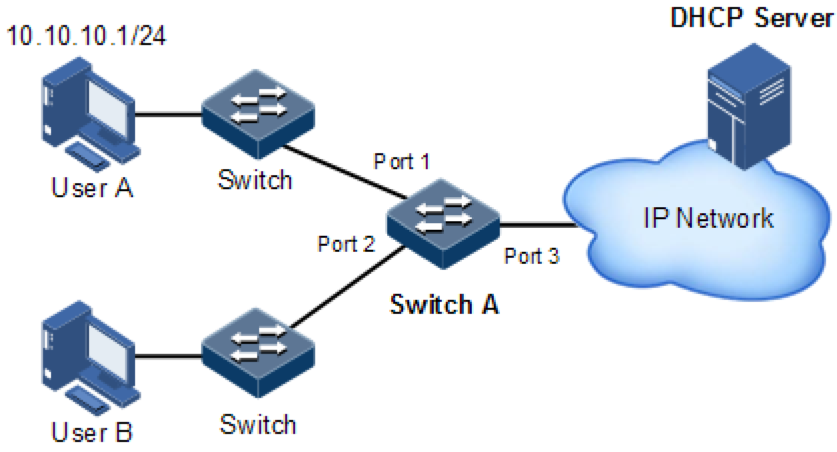
7.3.11 Example for configuring dynamic ARP inspection

Networking requirements

To prevent ARP attacks, configure dynamic ARP inspection on Switch A, as shown in Figure 7-4.

- Uplink Port 3 permits all ARP packets to pass.
- Downlink Port 1 permits ARP packets with specified IP address 10.10.10.1 to pass.
- Other interfaces permit ARP packets complying with dynamic binding learnt by DHCP Snooping to pass.
- Downlink Port 2 configures rate limiting on ARP packets. The rate threshold is set to 20 pps and recovery time for rate limiting is set to 15s.

Figure 7-4 Configuring dynamic ARP inspection



Configuration steps

Step 1 Set Port 3 to the trusted interface.

```
Qtech#config
Qtech(config)#interface port 3
Qtech(config-port)#ip arp-inspection trust
Qtech(config-port)#exit
```

Step 2 Configure static binding.

```
Qtech(config)#ip arp-inspection static-config
Qtech(config)#ip arp-inspection binding 10.10.10.1 port 1
```

Step 3 Enable dynamic ARP inspection binding.

```
Qtech(config)#ip dhcp snooping
Qtech(config)#ip arp-inspection dhcp-snooping
```

Step 4 Configure rate limiting on ARP packets on the interface.

```
Qtech(config)#interface port 2
Qtech(config-port)#ip arp-rate-limit rate 20
Qtech(config-port)#ip arp-rate-limit enable
Qtech(config-port)#exit
```

Step 5 Configure auto-recovery for rate limiting on ARP packets.

```
Qtech(config)#ip arp-rate-limit recover time 15
Qtech(config)#ip arp-rate-limit recover enable
```

Checking results

Use the **show ip arp-inspection** command to show configurations of interface trust status static/dynamic ARP binding.

```
Qtech#show ip arp-inspection
Static Config ARP Inspection: Enable
DHCP Snooping ARP Inspection: Enable
ARP Inspection Protect Vlan : 1-4094
Bind Rule Num            : 0
Vlan Acl Num             : ---
Remained Acl Num          : 512
Port   Trust
-------------
P1      no
P2      no
P3      yes
P4      no
P5      no
P6      no
……
P28     no
```

Use the **show ip arp-inspection binding** command to show information about the dynamic ARP binding table.

```
Qtech#show ip arp-inspection binding
Ip Address      Mac Address    VLAN  Port    Type         Inhw
---------------------------------------------------------------------
```

```
10.10.10.1      --            --      p1      static        yes
Current Rules Num: 1
History Max Rules Num: 1
```

Use the **show ip arp-rate-limit** command to show configurations of rate limiting on the interface and auto-recovery time for rate limiting.

```
Qtech#show ip arp-rate-limit
arp rate limit auto recover: enable
arp rate limit auto recover time: 15 second
Port   Enable-Status   Rate(Num/Sec)   Overload
--------------------------------------------------
1      Disabled       100           No
2      Enabled        20            Yes
3      Disabled       100           No
4      Disabled       100           No
5      Disabled       100           No
6      Disabled       100           No
```

7.4 RADIUS

7.4.1 Introduction

Remote Authentication Dial In User Service (RADIUS) is a standard communication protocol that authenticates remote access users intensively. RADIUS uses UDP as the transmission protocol (port 1812 and port 1813) which has a good instantaneity; at the same time, RADIUS supports retransmission mechanism and standby server mechanism which has a good reliability.

RADIUS authentication

RADIUS works in client/server mode. Network devices are clients of the RADIUS server. RADIUS server is responsible for receiving users' connection requests, authenticating uses, and replying configurations required by all clients to provide services for users. This mode can control users accessing devices and network to improve network security.

Clients and the RADIUS server communicate with each other through the shared key. The shared key is not transmitted through the network. In addition, any user password needs to be encapsulated when it is transmitted through clients and RADIUS. This helps prevent getting the user password by sniffing unsecure network.

RADIUS accounting

RADIUS accounting is used to authenticate users through RADIUS. When logging in, a user sends a starting account packet to the RADIUS accounting server, according to the accounting policy to send update packet to the RADIUS server. When logging off, the user sends a stopping account packet to the RADIUS accounting server, and the packet includes user online time. The RADIUS accounting server can record the access time and operations for each user through packets.

7.4.2 Preparing for configurations

Scenario

You can deploy the RADIUS server on the network to conduct authentication and accounting to control users to access to the QSW-8200 series switch and network. The QSW-8200 series switch can be used as agent of the RADIUS server, which authorizes user to access according to feedback from RADIUS.

Prerequisite

N/A

7.4.3 Default configurations of RADIUS

Default configurations of RADIUS are as below.

Function	Default value
RADIUS accounting	Disable
IP address of the RADIUS server	0.0.0.0
IP address of the RADIUS accounting server	0.0.0.0
Port ID of the RADIUS authentication server	1812
Port ID of the RADIUS accounting server	1813
Shared key communicated with the RADIUS accounting server	N/A
Policy for processing failed accounting	Online
Period for sending update packet	0

7.4.4 Configuring RADIUS authentication

Configure RADIUS authentication for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`interface ip`** *`if-number`*	Enter Layer 3 interface configuration mode.
3	`Qtech(config-ip)#`**`ip address`** *`ip-address`* `[` *`ip-mask`* `]` `[` *`vlan-list`* `]`	Configure the IPv4 address.
4	`Qtech(config-ip)#`**`end`**	Return privileged EXEC mode.

Step	Command	Description
5	`Qtech#radius [ backup ] ip-address [ auth-port port-number ]`	Assign an IP address and port ID for the RADIUS authentication server. Configure the **backup** parameter to assign the backup RADIUS authentication server.
6	`Qtech#radius-key string`	Configure the shared key for RADIUS authentication.
7	`Qtech#user login { local-radius | local-user | radius-local [ server-no-response ] | radius-user }`	Configure user login to be authenticated by RADIUS.
8	`Qtech#enable login { local-radius | local-user | radius-local [ server-no-response ] | radius-user }`	Configure RADIUS authentication mode for users to enter privileged EXEC mode.
9	`Qtech#enable auth { default | bypass | user }`	Configure the enable authentication mode for TACACS+ and RADIUS users.

7.4.5 Configuring RADIUS accounting

Configure RADIUS accounting for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#interface ip if-number`	Enter Layer 3 interface configuration mode.
3	`Qtech(config-ip)#ip address ip-address [ ip-mask ] [ vlan-list ]`	Configure the IPv4 address.
4	`Qtech(config-ip)#end`	Return privileged EXEC mode.
5	`Qtech#aaa accounting login enable`	Enable RADIUS accounting. Use the **aaa accounting login disable** command to disable this function.
6	`Qtech#radius [ backup ] accounting-server ip-address [ account-port ]`	Assign the IP address and UDP port ID for RADIUS accounting server. Configure parameter of backup to assign the backup RADIUS accounting server.
7	`Qtech#radius accounting-server key string`	Configure the shared key to communicate with the RADIUS accounting server, otherwise accounting will fail.
8	`Qtech#aaa accounting fail { offline | online }`	Configure policy for processing failed accounting.

Step	Command	Description
9	Qtech#**aaa accounting update** *period*	Configure the period for sending accounting update packets. If it is configured as 0, the system will never send accounting update packets. **Note** The RADIUS accounting server can record access time and operation for each user through accounting starting packets, update packets and finish packets.
10	Qtech#**aaa command authorize**{ **enable** | **disable** }	Enable/disable CLI for RADIUS authentication.
11	Qtech#**enable auth** { **default** | **bypass** | **user** }	Configure the enable authentication mode for TACACS+ and RADIUS users.

7.4.6 Checking configurations

Use the following commands to check configuration results.

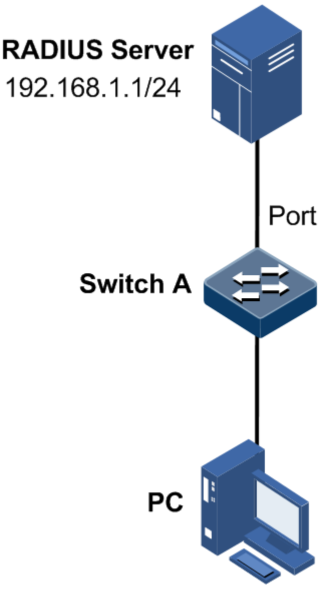
No.	Command	Description
1	Qtech#**show radius-server**	Show configurations of the RADIUS server.

7.4.7 Example for configuring RADIUS

Networking requirements

As shown in Figure 7-5, to control a user to access the Switch, you need to configure RADIUS authentication and accounting features on Switch A to authenticate login users on Switch A and record the operations. The period for sending update packets is 2 minutes. The user will be offline if accounting fails.

Figure 7-5 RADIUS networking



Configuration steps

Step 1 Configure authentication for login user through RADIUS.

```
Qtech#radius 192.168.1.1
Qtech#radius-key Qtech
Qtech#user login radius-user
Qtech#enable login local-radius
```

Step 2 Configure accounting for login user through RADIUS.

```
Qtech#aaa accounting login enable
Qtech#radius accounting-server 192.168.1.1
Qtech#radius accounting-server key Qtech
Qtech#aaa accounting fail offline
Qtech#aaa accounting update 2
```

Checking results

Use the **show radius-server** to show RADIUS configurations.

```
Qtech#show radius-server
Authentication server IP:      192.168.1.1 port:1812
Backup authentication server IP:0.0.0.0 port:1812
Authentication server key:     Qtech
Accounting server IP:         192.168.1.1 port:1813
Backup accounting server IP:   0.0.0.0 port:1813
```

```
Accounting server key:        Qtech
Accounting login:            enable
Update interval:             2
Accounting fail policy:        offline
```

7.5 TACACS+

7.5.1 Introduction

Terminal Access Controller Access Control System (TACACS+) is a kind of network access authentication protocol similar to RADIUS. The differences between them are:

- TACACS+ uses TCP port 49, which has higher transmission reliability compared with UPD port used by RADIUS.
- TACACS+ encrypts the holistic of packets except the standard head of TACACS+, and there is a field to show whether the data packets are encrypted in the head of packet. Compared to RADIUS user password encryption, the TACACS+ is much safer.
- TACACS+ authentication function is separated from authorization and accounting functions; it is more flexible in deployment.

In a word, TACACS+ is safer and more reliable than RADIUS. However, as an open protocol, RADIUS is more widely used.

7.5.2 Preparing for configurations

Scenario

You can authenticate and account on users by deploying a TACACS+ server on the network to control users to access the QSW-8200 series switch and network. TACACS+ is safer and more reliable than RADIUS. The QSW-8200 series switch can be used as an agent of the TACACS+ server, and authorize users access according to feedback result from the TACACS+ server.

Prerequisite

N/A

7.5.3 Default configurations of TACACS+

Default configurations of TACACS+ are as below.

Function	Default value
TACACS+ status	Disable
Login mode	local-user
IP address of the TACACS+ server	0.0.0.0, shown as "--"
IP address of the TACACS+ accounting server	0.0.0.0, shown as "--"

Function	Default value
Shared key communicated with the TACACS+ accounting server	N/A
Policy for processing failed accounting	Online
Period for sending update packets	0

7.5.4 Configuring TACACS+ authentication

Configure TACACS+ authentication for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface ip** *if-number*	Enter Layer 3 interface configuration mode.
3	Qtech(config-ip)#**ip address** *ip-address ip-mask vlan-id*	Configure the IPv4 address.
4	Qtech(config-ip)#**end**	Return to privileged EXEC mode.
5	Qtech#**tacacs-server** [**backup**] *ip-address* [**auth-port** *port-number*]	Assign an IP address for the TACACS+ authentication server. Configure the **backup** parameter to assign the backup TACACS+ authentication server.
6	Qtech#**tacacs-server key** *string*	Configure the shared key for TACACS+ authentication.
7	Qtech#**user login** { **local-tacacs** | **local-user** | **tacacs-local** [**server-no-response**] | **tacacs-user** }	Configure user login to be authenticated by TACACS+.
8	Qtech#**enable login** { | **local-tacacs** | **local-user** | **tacacs-local** [**server-no-response**] | **tacacs-user** }	Configure TACACS+ authentication mode for user to enter privileged EXEC mode.
9	Qtech#**enable auth** { **default** | **bypass** | **user** }	Configure mode for enable authentication of TACACS+ and RADIUS users.

7.5.5 Configuring TACACS+ accounting

Configure TACACS+ accounting for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.

Step	Command	Description
2	Qtech(config)#**interface ip** *if-number*	Enter Layer 3 interface configuration mode.
3	Qtech(config-ip)#**ip address** *ip-address ip-mask vlan-id*	Configure the IPv4 address.
4	Qtech(config-ip)#**end**	Return privileged EXEC mode.
5	Qtech#**aaa accounting login enable**	Enable TACACS+ accounting.
6	Qtech#**tacacs** [**backup**] **accounting-server** *ip-address* [*account-port*]	Assign an IP address for the TACACS+ accounting server. Configure the **backup** parameter to assign the backup TACACS+ accounting server.
7	Qtech#**tacacs-server key** *string*	Configure the shared key to communicate with the TACACS+ accounting server
8	Qtech#**aaa accounting fail** { **offline** | **online** }	Configure policy for processing failed accounting. By default, it is online, that is to allow login after accounting fails.
9	Qtech#**aaa accounting update** *period*	Configure the period for sending accounting update packets. If it is configured as 0, the system never sends accounting update packets. By default, the period is 0.
10	Qtech#**aaa command authorize**{ **enable**| **disable** }	Enable/Disable the function of conducting TACACS+ through CLI.
11	Qtech#**enable auth** { **default** | **bypass** | **user** }	Configure mode for enable authentication of TACACS+ and RADIUS users.

7.5.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show tacacs-server**	Show TACACS+ server configuration.
2	Qtech#**show radius-server**	Show TACACS+ accounting configuration. **Note** Use the **show radius-server** command to show configurations of TACACS+ accounting and RADIUS accounting. By default, the authentication information is RADIUS authentication configuration.

7.5.7 Maintenance

Maintain the QSW-8200 series switch as below.

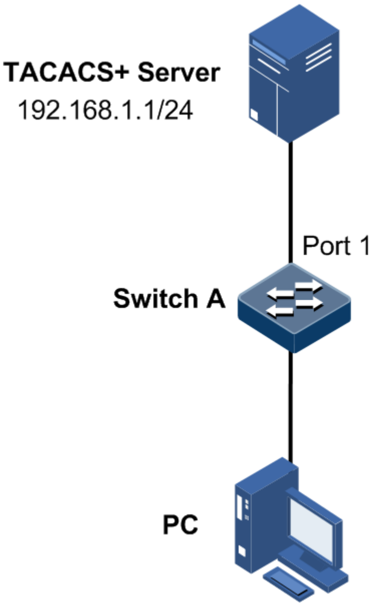
Command	Description
`Qtech#clear tacacs statistics`	Clear TACACS+ statistics.

7.5.8 Example for configuring TACACS+

Networking requirements

As shown in Figure 7-6, configure TACACS+ authentication on Switch A to authenticate login user and control users from accessing the QSW-8200 series switch.

Figure 7-6 TACACS+ networking



Configuration steps

Configure user login authentication through TACACS+.

```
Qtech#tacacs-server 192.168.1.1
Qtech#tacacs-server key Qtech
Qtech#user login tacacs-user
Qtech#enable login local-tacacs
```

Checking results

Use the **show tacacs-server** command to show TACACS+ configurations.

```
Qtech#show tacacs-server
Server Address:         192.168.1.1     port:  --
Backup Server Address:           --     port:  --
Server Shared Key:    Qtech
Accounting server Address:       --     port:  --
Backup Accounting server Address:  --     port:  --
Total Packet Sent:   0
Total Packet Recv:   0
Num of Error Packets: 0
```

7.6 802.1x

7.6.1 Introduction

802.1x, based on IEEE 802.1x, is a VLAN-based network access control technology. It is used to solve authentication and security problems for LAN users.

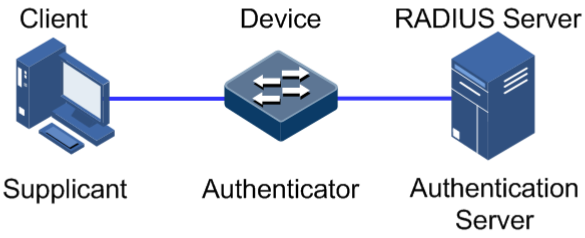
It is used to authenticate and control access devices at the physical layer of the network device. It defines a point-to-point connection mode between the device interface and user devices. User devices, connected to the interface, can access resources in the LAN if they are authenticated. Otherwise, they cannot access resources in the LAN through the QSW-8200 series switch.

802.1x structure

As shown below, 802.1x authentication uses Client/Server mode, including the following three parts:

- Supplicant: the device installed with 802.1x client (such as Windows XP 802.1x client) at the client side, such as a PC
- Authenticator: the access control device providing 802.1x feature, such as a switch
- Authentication server: a device used for authenticating, authorizing, and accounting users. In general, the RADIUS server is taken as the 802.1x authentication server

Figure 7-7 802.1x structure



802.1x access control mode

The QSW-8200 series switch supports three access control modes:

- Authorized-force: the interface is always in authorized status, and any user can visit network resources without authentication.
- Unauthorized-force: interface is always in unauthorized status, and any user cannot visit network resources.

- Auto: permit user authentication. Passed user can visit network resources.

802.1x Authentication method

The QSW-8200 series switch supports the following two authentication methods:

- Portbased authentication: after the first user connected to one interface successfully authorized, other users on this interface do not have to be authenticated.
- Macbased authentication: forbid multiple users on the same interface from using the same account to visit network resources. Only the last authorized user can visit the network resources.

802.1x timer

The 802.1x protocol includes the following timers:

- Request/Identity request packet timeout timer (imer tx-period): the Request/Identity request packet is sent by the QSW-8200 series switch to the user, and it is used to request account user name. The device will start this timer after request packet is sent out. If no respond packet is received during this period, the QSW-8200 series switch will resend the request packet.
- Request/MD5 Challenge request packet timeout timer (timer supp-timeout): the Request/MD5 Challenge request packet is sent by the QSW-8200 series switch to the user, and it is used for transmitting encryption code. The device starts this timer after sending the request packet. If no respond packet is received during this period, the QSW-8200 series switch will resent the request packet.
- RADIUS server timeout timer (timer server-timeout): after the QSW-8200 series switch sends the request packet to the RADUIS server, it starts this timer. If no respond packet is received during this time period, the QSW-8200 series switch will resend the request packet.
- Silence timer (timer quiet-period): if user authentication fails, the QSW-8200 series switch will keep silence for a while. During this period, the QSW-8200 series switch will ignore all authentication requests from this user.
- Reauthentication timer (timer reauth-period): if the QSW-8200 series switch is enabled with reauthentication, the QSW-8200 series switch will restart authentication to all users on the interface periodically.

7.6.2 Preparing for configurations

Scenario

The Dot1x feature can authenticate users on the interface, and manage users to access network resources.

Prerequisite

If the RADIUS server is needed during 802.1x authentication,

- Configure the IP address and public key of the RADUIS server.
- The QSW-8200 series switch can ping through the RADIUS server successfully.

7.6.3 Default configurations of Dot1x

Default configurations of Dot1x are as below.

Function	Default value
Global 802.1x status	Disable
Interface 802.1x status	Disable
Authentication control mode	Auto
Authentication method	portbased
Reauthentication status	Disable
Request/Identity request packet timeout timer (timer tx-period)	30s
Request/MD5 Challenge request packet timout timer (timer supp-timeout)	30s
RADIUS server timeout timer (timer server-timeout)	100s
Silence timer (timer quiet-period)	60s
Reauthentication timer (timer reauth-period)	3600s

7.6.4 Configuring basic functions of 802.1x

Enabling 802.1x

Enable 802.1x for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`dot1x enable`**	Enable global 802.1x.
3	`Qtech(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
4	`Qtech(config-port)#`**`dot1x enable`**	Enable interface 802.1x.

Configuring access control mode

Configure access control mode for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.

Step	Command	Description
3	Qtech(config-port)#**dot1x auth-control** { **auto** | **authorized-force** | **unauthorized-force** }	Configure access control mode on the interface.

Configuring access authentication method

Configure access authentication method for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**dot1x auth-method** { **macbased** | **portbased** }	Configure access authentication method.

Enabling reauthentication

If enabled with reauthentication on the interface, the QSW-8200 series switch authenticates user on the interface periodically, to detect the status change of users on the interface.

Configure reauthentication for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**dot1x reauthentication enable**	Enable reauthentication.

7.6.5 (Optional) configuring 802.1x timer

Configure the 802.1x timer for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**dot1x timer tx-period** *second*	Configure the Request/Identity request packet timeout timer.

Step	Command	Description
4	Qtech(config-port)#**dot1x timer supp-timeout** *second*	Configure the Request/MD5 Challenge request packet timeout timer.
5	Qtech(config-port)#**dot1x timer server-timeout** *second*	Configure the RADIUS server timeout timer.
6	Qtech(config-port)#**dot1x timer quiet-period** *second*	Configure the silence timer.
7	Qtech(config-port)#**dot1x timer reauth-period** *second*	Configure the reauthentication timer.

7.6.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show dot1x port-list** *port-list*	Show 802.1x configurations on the interface.
2	Qtech#**show dot1x port-list** *port-list* **statistics**	Show 802.1x statistics on the interface.
3	Qtech#**show dot1x port-list** *port-list* **user**	Show information dynamically sent by the interface.
4	Qtech#**show radius-server**	Show configurations of the RADIUS server.

7.6.7 Maintenance

Maintain the QSW-8200 series switch as below.

Command	Description
Qtech(config)#**clear dot1x port-list** *port-list* **statistics**	Clear statistics of EAPOL packets on the interface.

7.6.8 Example for configuring 802.1x

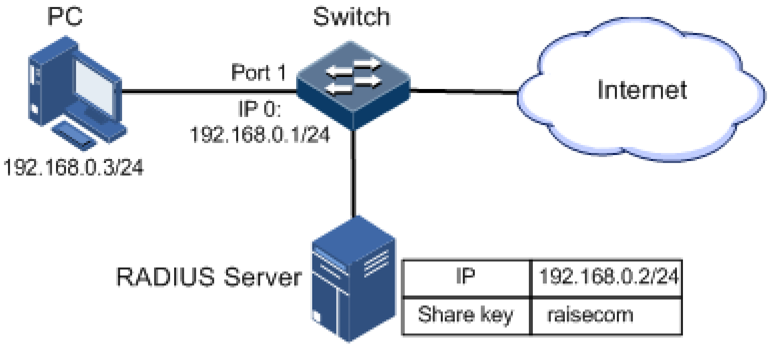
Networking requirements

As shown in Figure 7-8, the network administrator configures 802.1x to control the PC to access the Internet.

- The PC passing RADIUS server authentication can visit internet.
- The PC can visit internet without authentication in authorized-force mode.

- The PC cannot visit internet in unauthorized-force mode.
- After the PC passes authentication, the Switch will start reauthentication every 600s.

Figure 7-8 Dot1x networking



Configuration steps

Step 1 Add an account with the use name as user1 and password as 123 on the RADIUS server

Step 2 Configure the IP address of the Switch.

```
Qtech#config
Qtech(config)#interface ip 0
Qtech(config-ip)#ip address 192.168.0.1 255.255.255.0 1
Qtech(config-ip)#end
```

Step 3 Configure the IP address and public key of the RADIUS server.

```
Qtech#radius 192.168.0.2
Qtech#radius-key Qtech
```

Step 4 Enable global and interface 802.1x.

```
Qtech#config
Qtech(config)#dot1x enable
Qtech(config)#interface port 1
Qtech(config-port)#dot1x enable
```

Step 5 The client on PC starts authentication request, with username user1 and password 123. The client APP shows that authentication is successful, and the PC can access the Internet.

Step 6 Configure interface in authorized-force mode, and the PC can visit internet without authentication.

```
Qtech(config-port)#dot1x auth-control authorized-force
```

Step 7 Configure the interface as unauthorized-force mode, and the PC cannot access the Internet regardless that it uses correct username and password or not.

```
Qtech(config-port)#dot1x auth-control unauthorized-force
```

Step 8 Enable reauthentication, and set the timer as 600s.

```
Qtech(config-port)#dot1x reauthentication enable
Qtech(config-port)#dot1x timer reauth-period 600
Qtech(config-port)#end
```

Checking results

Show 802.1x configurations on the interface.

```
Qtech#show dot1x port-list 1
802.1x Global Admin State: enable
Port port1
--------------------------------------------------------
  802.1X Port Admin State:    Enable
  PAE:                    Authenticator
  PortMethod:              Portbased
  PortControl:              ForceUnauthorized
  PortStatus:              Authorized
  Authenticator PAE State:    Initialize
  Backend Authenticator State: Initialize
  ReAuthentication:          Enable
  QuietPeriod:              60(s)
  ServerTimeout:            100(s)
  SuppTimeout:              30(s)
  ReAuthPeriod:             600(s)
  TxPeriod:                30(s)
```

Show configurations of the RADIUS server.

```
Qtech#show radius-server
Authentication server IP:      192.168.0.2 port:1812
Backup authentication server IP:0.0.0.0 port:1812
Authentication server key:     Qtech
Accounting server IP:         0.0.0.0 port:1813
Backup accounting server IP:   0.0.0.0 port:1813
Accounting server key:
```

```
Accounting login:            disable
Update interval(min.):        0
Accounting fail policy:       online
```

7.7 PPPoE+

7.7.1 Introduction

In security domain on the Internet, Point to Point Protocol Over Ethernet (PPPoE) is a widely used access security mechanism.

PPPoE is widely used in Broadband Access Authentication Dial. Packets sent from a PPPoE client contain user information, which causes account sharing and theft.

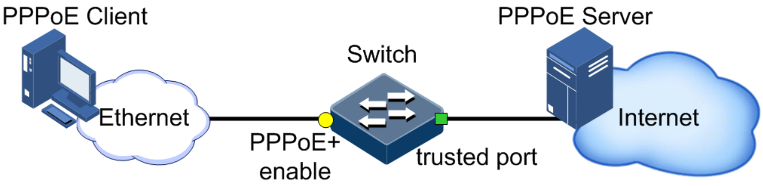
PPPoE Intermediate Agent (PPPoE+) is an enhancement to PPPoE functionality. It is used to process authentication packets. PPPoE+ adds device information in authentication packets, and binds the account with the access device. This provides the server with enough information to identify user, avoids account sharing and theft, and protects the interest of the carrier and illegal users.

Principle

Figure 7-9 shows PPPoE+ networking.

On the Switch, enable PPPoE+ on the client side interface, set the interface connected to PPPoE server as the trusted interface. When the Switch receives a PPPoE protocol packet sent from the client, the Switch will add information about its own (device type and interface number) in the protocol packet. Thus, the server can manage the client according to the information in the packet. Meanwhile, the PPPoE authentication packet is only forwarded between the PPPoE+ client interface and trusted interface, which can prevent client cheat and server cheat.

Figure 7-9 PPPoE+ networking



Processing PPPoE packets

PPPoE+ processes particular Tag in PPPoE packet, including Circuit ID and Remote ID, and adds device information about binding user account and access device.

There are two kinds of padding pattern of Circuit: Switch mode and ONU mode. The default mode is Switch mode.

Table 7-1 describes Circuit ID padding information.

Table 7-1 Circuit ID padding information

Mode	Action	Padding information
Switch mode	By default, no attach-string is configured, and no Circuit Id is configured.	Interface number/VLAN/device hostname
	The attach-string is configured, but no Circuit ID is configured.	Interface number/VLAN/attach-string
	The Circuit Id is configured.	Customized Circuit ID
ONU mode	Read-only	0 0/0/0: 0.0 0/0/0/0/0/0/MAC 0/0/Port: eth/4096.CVLAN LN

Note

- Only when the interface work as an ONU, it is in ONU mode; otherwise, it is in Switch mode.
- Circuit ID is fixed and read-only in ONU mode. Only in Switch mode, it is configurable.
- In the above, "Interface number/VLAN/device host name" refers to the interface connected to the client.

The Remote ID is padded with a MAC address. You can select to use the MAC address of the Switch or client, and in the form of binary or ASCII.

Tag overwriting

For some reason, some Tags in PPPoE packet may be forged. For security, PPPoE+ will overwrite the original Tag with the correct one. The specific processing principles are shown in Table 7-2.

Table 7-2 Method for processing original Tag of packets

Overwrite	Input packet	Output packet
Enable	With Tag	Delete the original Tag, and add new Tag at the end of the packet.
	No Tag	Add a new Tag at the end of the packet.
Disable	With Tag	No change
	No Tag	Add a new Tag at the end of the packet.

7.7.2 Preparing for configurations

Scenario

To prevent illegal clients from accessing during PPPoE authentication, you can configure PPPoE+ to add device information in PPPoE protocol packets for network security.

Prerequisite

N/A

7.7.3 Default configurations of PPPoE+

Default configurations of PPPoE+ are as below.

Function	Default value
Global PPPoE+ status	Disable
Interface PPoE+ status	Disable
Circuit ID padding mode	Switch Mode: • Circuit ID information: interface number/VLAN/attach-string • Circuit ID attach-string: device hostname
Remote ID padding MAC address	Device MAC
Remote ID padding form	Binary
Interface trust status	Untrust
Tag overwriting	Disable

Note

By default, PPPoE packet can be forwarded through the interface without being added with extra information.

7.7.4 Enabling PPPoE+

Enable PPPoE+ for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`pppoeagent enable`**	Enable global PPPoE+.
3	`Qtech(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
4	`Qtech(config-port)#`**`pppoeagent enable`**	Enable interface PPPoE+. The interface connected to the client should be enabled with PPPoE+.

7.7.5 Configuring PPPoE+ trusted interface

Configure the PPPoE+ trusted interface for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#interface port port-id`	Enter physical layer interface configuration mode.
3	`Qtech(config-port)#pppoeagent trust`	Configure the PPPoE+ trusted interface. The interface connected to PPPoE server should be a trusted interface.

7.7.6 Configuring Circuit ID

Configure the Circuit ID for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#pppoeagent circuit-id mode { onu | switch }`	Configure Circuit ID padding mode.
3	`Qtech(config)#pppoeagent circuit-id { attach-string | format | hex } string`	(Optional) configure Circuit ID attach-string. By default, attach-string is the device hostname. You can use this command to redefine this string.
4	`Qtech(config)#pppoeagent circuit-id mac-format string`	(Optional) configure attached string of Circuit ID. Circuit ID contains a host name hostname as an attached string. You can configure the customized attached string by using this command.
4	`Qtech(config)#interface port port-id`	Enter physical layer interface configuration mode.
5	`Qtech(config-port)#pppoeagent circuit-id string`	(Optional) configure the Circuit ID as customized string. Configure this feature on the interface connected to the client.

7.7.7 Configuring Remote ID

Configure the Remote ID for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#interface port port-id`	Enter physical layer interface configuration mode.

Step	Command	Description
3	Qtech(config-port)#**pppoeagent remote-id { client-mac | switch-mac }**	(Optional) configure the MAC address of Remote ID padding for PPPoE+ on the interface. Configure this feature on interface connected to the client.
4	Qtech(config-port)#**pppoeagent remote-id format { ascii | binary }**	(Optional) configure Remote ID padding mode for PPPoE+ on the interface. Configure this feature on the interface connected to the client.

7.7.8 Enabling vendor-tag overwriting

Configure vendor-tag overwriting for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**pppoeagent vendor-specific-tag overwrite enable**	Enable Tag overwriting. Configure this feature on the interface connected to the client.

7.7.9 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show pppoeagent** [**port-list** *port-list*]	Show PPPoE+ configurations.
2	Qtech#**show pppoeagent statistic** [**port-list** *port-list*]	Show PPPoE+ statistics.

7.7.10 Maintenance

Maintain the QSW-8200 series switch as below.

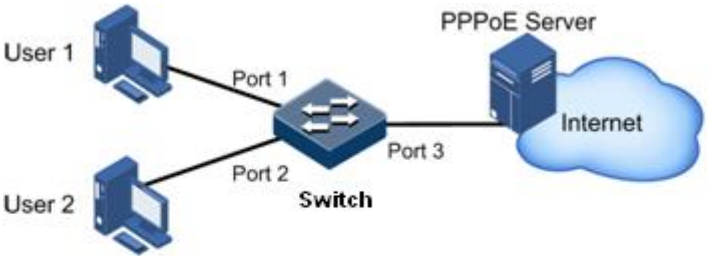
Command	Description
Qtech(config)#**clear pppoeagent statistic** [**port-list** *port-list*]	Clear PPPoE+ statistics.

7.7.11 Example for configuring PPPoE+

Networking requirements

As shown in Figure 7-10, to prevent illegal clients from accessing and managing legal users, you can configure PPPoE+ on the Switch.

Figure 7-10 PPPoE+ networking



Configuration steps

Step 1 Enable PPPoE+ on the interface at the client side.

```
Qtech#config
Qtech(config)#pppoeagent enable
Qtech(config)#interface port 1
Qtech(config-port)#pppoeagent enable
Qtech(config-port)#exit
Qtech(config)#interface port 2
Qtech(config-port)#pppoeagent enable
```

Step 2 Configure Circuit ID and Remote ID.

```
Qtech(config)#pppoeagent circuit-id attach-string Qtech
Qtech(config)#interface port 1
Qtech(config-port)#pppoeagent circuit-id user01
Qtech(config-port)#exit
Qtech(config)#interface port 2
Qtech(config-port)#pppoeagent remote-id client-mac
Qtech(config-port)#pppoeagent remote-id format ascii
Qtech(config-port)#exit
```

Step 3 Enable Tag overwriting on client side interface.

```
Qtech(config)#interface port 1
Qtech(config-port)#pppoeagent vendor-specific-tag overwrite enable
Qtech(config-port)#exit
```

Step 4 Configure the interface connected to the server as the trusted interface

```
Qtech(config)#interface port 3
Qtech(config-port)#pppoenagent trust
Qtech(config-port)#exit
```

Checking results

Use the **show pppoeagent** command to show PPPoE+ configurations.

```
Qtech#show pppoeagent port-list 1-2
Global PPPoE+ status: enable
Attach-string: Qtech
Circuit ID padding mode: switch
Port   State   Overwrite  Remote-ID   Format-rules  Circuit-ID
----------------------------------------------------------------
P1   enable  enable    switch-mac   binary      user01
P2   enable  disable   client-mac   ASCII       %default%

**In switch mode, Circuit-ID's default string is: Port\Vlan\Attach-string.
**In onu mode, Circuit-ID's default string is: 0 0/0/0:0.0
0/0/0/0/0/0/MAC 0/0/Port:eth/4096.CVLAN LN.
**Attach-string's default string is the hostname.
Qtech#show pppoeagent port-list 3
Global PPPoE+ status: enable
Attach-string: Qtech
Circuit ID padding mode: switch
Port   State   Overwrite  Remote-ID   Format-rules  Circuit-ID
----------------------------------------------------------------
P3   trust   disable   switch-mac   binary      %default%

**In switch mode, Circuit-ID's default string is: Port\Vlan\Attach-string.
**In onu mode, Circuit-ID's default string is: 0 0/0/0:0.0
0/0/0/0/0/0/MAC 0/0/Port:eth/4096.CVLAN LN.
**Attach-string's default string is the hostname.
```

7.8 Storm control

7.8.1 Introduction

The Layer 2 network is a broadcast domain. When an interface receives excessive broadcast, unknown multicast, and unknown unicast packets, broadcast storm occurs. If you do not control broadcast packets, broadcast storm may occur and occupies much network bandwidth. Broadcast storm can degrade network performance and impact forwarding of unicast packets or even lead to communication halt.

Restricting broadcast flow generated from network on Layer 2 device can suppress broadcast storm and ensure common unicast forwarding normally.

Occurrence of broadcast storm

The following flows may cause broadcast flow:

- Unknown unicast packets: unicast packets of which the destination MAC is not in the MAC address table, namely, the Destination Lookup Failure (DLF) packets. If these packets are excessive in a period, the system floods them and broadcast storm may occur.
- Unknown multicast packets: the destination MAC address is not in the MAC address table. Layer 2 devices broadcast this type of traffic.
- Broadcast packets: packets of which the destination MAC is a broadcast address. If these packets are excessive in a period, broadcast storm may occur.

Principle of storm control

The storm control allows the interface to filter broadcast, unknown multicast, unknown unicast packets that may generate broadcast storm on the network. After storm control is enabled, when the packets received by a device are accumulated to a preconfigured threshold, the device will automatically discard broadcast packets. If storm control is disabled or broadcast packets have not reached the preconfigured threshold, the device will normally forward packets to other interfaces of the device.

For example, the threshold for storm control is 1024 pps; broadcast packets, unknown unicast packets, and unknown multicast packets are limited to 1024 pps. If one type of packets exceeds this threshold, this type of packets is discarded.

7.8.2 Preparing for configurations

Scenario

Configuring storm control in Layer 2 network can control the broadcast storm when the broadcast packets increase in network and then ensure unicast packets to be forwarded normally.

Prerequisite

- Connect interfaces.
- Configure physical parameters to make interfaces Up at the physical layer.

7.8.3 Default configurations of storm control

Default configurations of storm control are as below.

Function	Default value
Storm control status of broadcast packets	Enable
Storm control status of multicast packets and unicast packets	Disable
Storm control status of unknown unicast packets	Disable
Storm control threshold	1024 pps

7.8.4 Configuring storm control

Enable storm control for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#storm-control { broadcast | dlf | multicast } enable port-list port-list`	Enable storm control on a specified interface.
3	`Qtech(config)#storm-control pps value`	Configure threshold for storm control.

7.8.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Qtech#show storm-control`	Show configurations of storm control.

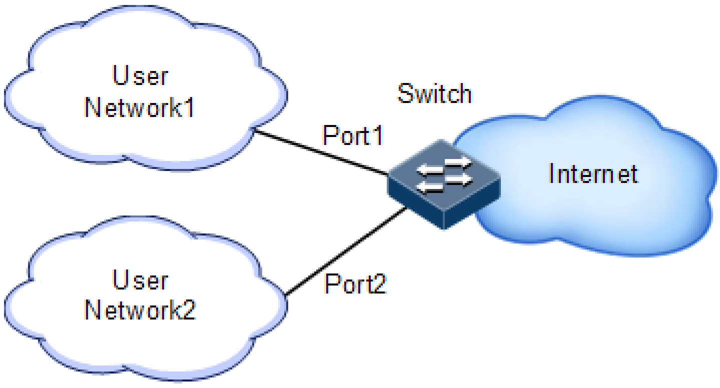
7.8.6 Example for configuring storm control

Networking requirements

As shown in Figure 7-11, when port 1 and port 2 on the Switch receive excessive unknown unicast packets or broadcast packets, the Switch forwards these packets to all interfaces except the receiving interface, which may cause broadcast storm and lower forwarding performance of the Switch.

To restrict influence on the Switch caused by broadcast storm, you need to configure storm control on the Switch to control broadcast packets and unknown unicast packets from user networks 1 and 2, with the threshold of 640 pps.

Figure 7-11 Storm control networking



Configuration steps

Step 1 Configure storm control over broadcast packets on port 1 and port 2.

```
Qtech#config
Qtech(config)#storm-control broadcast enable port-list 1
Qtech(config)#storm-control broadcast enable port-list 2
```

Step 2 Configure storm control over unknown unicast packets on port 1 and port 2.

```
Qtech(config)#storm-control dlf enable port-list 1
Qtech(config)#storm-control dlf enable port-list 2
```

Step 3 Configure the threshold for storm control.

```
Qtech(config)#storm-control pps 640
```

Checking results

Use the **show storm-control** command to show configurations of storm control.

```
Qtech#show storm-control
Threshold: 640 pps
Interface      Broadcast      Multicast      Unicast
-----------------------------------------------------------
P1            Enable       Disable        Enable
P2            Enable       Disable        Enable
P3            Enable       Disable       Disable
......
```

7.9 IP Source Guard

7.9.1 Introduction

IP Source Guard uses a binding table to defend against IP Source spoofing and solve IP address embezzlement without identity authentication. IP Source Guard can cooperate with DHCP Snooping to generate dynamic binding. In addition, you can configure static binding manually. DHCP Snooping filters untrusted DHCP packets by establishing and maintaining the DHCP binding database.

IP Source Guard binding entry

IP Source Guard is used to match packet characteristics, including source IP address, source MAC address, and VLAN tags, and can support the interface to combine with the following characteristics (hereinafter referred to as binding entries):

- Interface+IP
- Interface+IP+MAC
- Interface+IP+VLAN
- Interface+IP+MAC+VLAN

According to the generation mode of binding entries, IP Source Guard can be divided into static binding and dynamic binding:

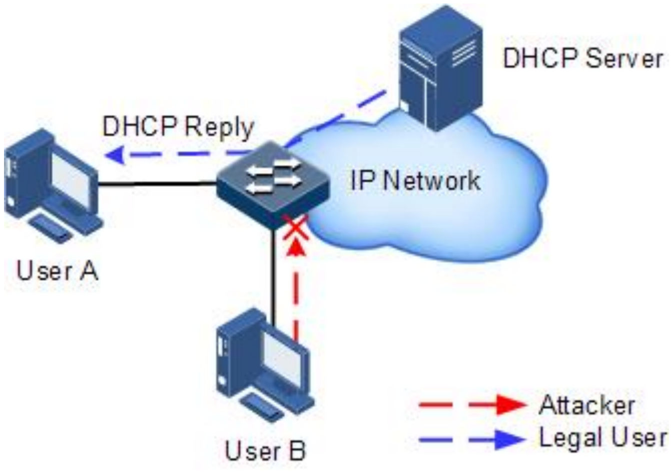
- Static binding: configure binding information manually and generate binding entry to complete the interface control, which fits for the case where the number of hosts is small or where you need to perform separate binding on a single host.
- Dynamic binding: obtain binding information automatically from DHCP Snooping to complete the interface control, which fits for the case where there are many hosts and you need to adopt DHCP to perform dynamic host configurations. Dynamic binding can effectively prevent IP address conflict and embezzlement.

Principle of IP Source Guard

The principle of IP Source Guard is to build an IP source binding table within the QSW-8200 series switch. The IP source binding table is taken as the basis for each interface to test received data packets. Figure 7-12 shows the principle of IP Source Guard.

- If the received IP packets meet the relationship of Port/IP/MAC/VLAN binding entries in IP source binding table, forward these packets.
- If the received IP packets are DHCP data packets, forward these packets.
- Otherwise, discard these packets.

Figure 7-12 Principle of IP Source Guard



Before forwarding IP packets, the QSW-8200 series switch compares the source IP address, source MAC address, interface ID, and VLAN ID of the IP packets with binding table information. If the information matches, it indicates that the user is legal and the packets are permitted to forward normally. Otherwise, the user is an attacker and the IP packets are discarded.

7.9.2 Preparing for configurations

Scenario

There are often some IP source spoofing attacks on the network. For example, the attacker forges legal users to send IP packets to the server, or the attacker forges the source IP address of another user to communicate. This makes the legitimate users cannot get network services normally.

With IP Source Guard binding, you can filter and control packets forwarded by the interface, prevent the illegal packets from passing through the interface, thus to restrict the illegal use of network resources and improve the interface security.

Prerequisite

Enable DHCP Snooping before if there is a DHCP user.

7.9.3 Default configurations of IP Source Guard

Default configurations of IP Source Guard are as below.

Function	Default value
IP Source Guide static binding	Disable
IP Source Guide dynamic binding	Disable
Interface trust status	Untrusted

7.9.4 Configuring interface trust status of IP Source Guard

Configure interface trust status of IP Source Guard for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Qtech(config-port)#`**`ip verify source trust`**	(Optional) configure the interface to a trusted interface. Use the **no ip verify source trust** command to configure the interface to an untrusted interface. In this case, all packets, but for DHCP packets and IP packets that meet binding, are not forwarded. When the interface is in trusted status, all packets are forwarded normally.

7.9.5 Configuring interface trust status of IPv6 Source Guard

Configure interface trust status of IPv6 Source Guard for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**ipv6 verify source trust**	(Optional) configure the interface to a trusted interface. Use the **no ipv6 verify source trust** command to configure the interface to an untrusted interface. In this case, all packets, but for DHCP packets and IP packets that meet binding, are not forwarded. When the interface is in trusted status, all packets are forwarded normally.

7.9.6 Configuring IP Source Guide binding

Configuring IP Source Guide static binding

Configure IP Source Guide static binding for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**ip verify source**	Enable static IP Source Guide binding.
3	Qtech(config)#**ip source binding** *ip-address* [*mac-address*] [**vlan** *vlan-id*] **port** *port-id*	Configure static binding. Use the **no ip source binding** *ip-address* command to delete the static binding.

Note

- The configured static binding does not take effect when global static binding is disabled. Only when global static binding is enabled, the static binding takes effect.
- For an identical IP address, the manually-configured static binding will cover the dynamic binding. However, it cannot cover the existing static binding. When the static binding is deleted, the system will recover the covered dynamic binding automatically.

Configuring IP Source Guide dynamic binding

Configure IP Source Guide dynamic binding for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#ip verify source dhcp-snooping`	Enable IP Source Guide dynamic binding.

Note

- The dynamic binding learnt through DHCP Snooping does not take effect when global dynamic binding is disabled. Only when global dynamic binding is enabled can the dynamic binding take effect.
- If an IP address exists in the static binding table, the dynamic binding does not take effect. In addition, it cannot cover the existing static binding.

Configuring binding translation

Configure binding translation for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#ip verify source dhcp-snooping`	Enable IP Source Guide dynamic binding.
3	`Qtech(config)#ip source binding dhcp-snooping static`	Translate the dynamic binding to the static binding.
4	`Qtech(config)#ip source binding auto-update`	(Optional) enable auto-translation. After it is enabled, dynamic binding entries learned through DHCP Snooping are directly translated into static binding entries. Use the **no ip source binding auto-update** command to disable auto-translation into static entries.

7.9.7 Configuring IPv6 Source Guide binding

Configuring IPv6 Source Guide static binding

Configure IPv6 Source Guide static binding for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.

Step	Command	Description
2	Qtech(config)#**ipv6 verify source**	Enable static IPv6 Source Guide binding.
3	Qtech(config)#**ipv6 source binding** *ipv6-address* [*mac-address*] [**vlan** *vlan-id*] **port** *port-id*	Configure static binding. Use the **no ipv6 source binding** *ip-address* command to delete the static binding.

Note

- The configured static binding does not take effect when global static binding is disabled. Only when global static binding is enabled, the static binding takes effect.
- For an identical IPv6 address, the manually-configured static binding will cover the dynamic binding. However, it cannot cover the existing static binding. When the static binding is deleted, the system will recover the covered dynamic binding automatically.

Configuring IPv6 Source Guide dynamic binding

Configure IPv6 Source Guide dynamic binding for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**ipv6 verify source dhcp-snooping**	Enable IPv6 Source Guide dynamic binding.

Note

- The dynamic binding learnt through DHCP Snooping does not take effect when global dynamic binding is disabled. Only when global dynamic binding is enabled can the dynamic binding take effect.
- If an IPv6 address exists in the static binding table, the dynamic binding does not take effect. In addition, it cannot cover the existing static binding.

Configuring binding translation

Configure binding translation for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**ipv6 verify source dhcp-snooping**	Enable IPv6 Source Guide dynamic binding.

Step	Command	Description
3	Qtech(config)#**ipv6 source binding dhcp-snooping static**	Translate the dynamic binding to the static binding.
4	Qtech(config)#**ipv6 source binding auto-update**	(Optional) enable auto-translation of IPv6 into static entries. After it is enabled, dynamic binding entries learned through DHCP Snooping are directly translated into static binding entries. Use the **no ipv6 source binding auto-update** command to disable auto-translation into static entries.

7.9.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show ip verify source**	Show global binding status and interface trusted status.
2	Qtech#**show ip source binding [port** *port-id* **]**	Show configurations of IP Source Guard binding, interface trusted status, and binding table.
3	Qtech#**show ipv6 source binding [port** *port-id* **]**	Show information about IPv6 Source Guard binding.
4	Qtech#**show ipv6 verify source**	Show global IPv6 binding status and interface trust status.

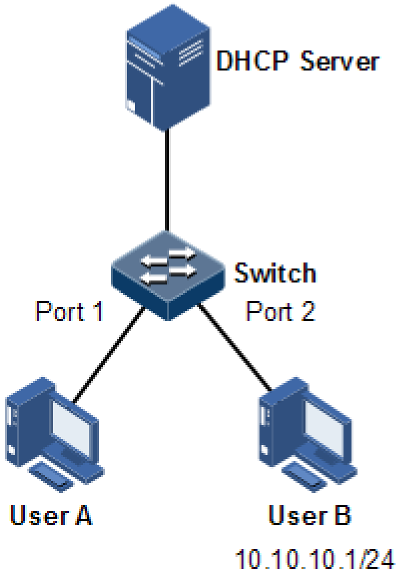
7.9.9 Example for configuring IP Source Guard

Networking requirements

As shown in Figure 7-13, to prevent IP address embezzlement, you need to configure IP Source Guard on the switch.

- The Switch permits all IP packets on Port 1 to pass.
- Port 2 permits IP packets with specified the IP address 10.10.10.1 and subnet mask 255.255.255.0 and the IP packets meeting DHCP Snooping learnt dynamic binding to pass.
- Other interfaces only permit the packets meeting DHCP Snooping learnt dynamic binding to pass.

Figure 7-13 Configuring IP Source Guard



Configuration steps

Step 1 Set Port 1 to a trusted interface.

```
Qtech#config
Qtech(config)#interface port 1
Qtech(config-port)#ip verify source trust
Qtech(config-port)#exit
```

Step 2 Configure static binding.

```
Qtech(config)#ip verify source
Qtech(config)#ip source binding 10.10.10.1 port 2
```

Step 3 Enable global dynamic IP Source Guard binding.

```
Qtech(config)#ip verify source dhcp-snooping
```

Checking results

Use the **show ip source binding** command to show configurations of the static binding table.

```
Qtech#show ip source binding
History Max Entry Num: 1
```

```
Current Entry Num: 1
Ip Address       Mac Address     VLAN   Port      Type      Inhw
----------------------------------------------------------------
10.10.10.1       --            --     P2     static    yes
```

Use the **show ip verify source** command to show interface trusted status and configurations of IP Source Guard static/dynamic binding.

```
Qtech#show ip verify source
Static Bind: Enable
Dhcp-Snooping Bind: Enable
Port     Trust
-----------------
P1     yes
P2     no
P3     no
P4     no
P5     no
P6     no
…
```

8 Reliability

This chapter describes basic principles and configurations of reliability, and provides related configuration examples, including the following sections:

- Link aggregation
- Interface backup
- ELPS (G.8031)
- ERPS (G.8032)
- Failover

8.1 Link aggregation

8.1.1 Introduction

With link aggregation, multiple physical Ethernet interfaces are combined to form a Logical Aggregation Group (LAG). Multiple physical links in one LAG are taken as a logical link. The link aggregation helps share traffics among members in an LAG. Link aggregation not only effectively improves reliability of links between devices, but also helps gain higher bandwidth without upgrading hardware.

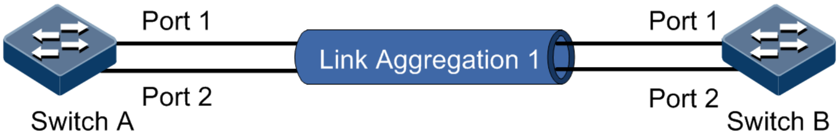
Every physical interface in the LAG is called the member interface, and the aggregated logical interface is called the trunk interface.

Link aggregation is the most widely used and most simple function in Ethernet reliability technology.

Advantage of link aggregation

As shown in Figure 8-1, Switch A and Switch B have two physical links between them. These two links are grouped together and form a logical link aggregation 1.

Figure 8-1 Link aggregation



Logical Link Aggregation 1 has the following advantages:

- Higher reliability: all the members in the LAG keep standby for others. If one link becomes Down, the others can carry the traffic of the Down one immediately.
- Higher bandwidth: you need not to upgrade the existing hardware to obtain a higher throughput bandwidth. By combining several physical links, the LAG can provide a higher bandwidth based on bandwidth summary of all the physical links.
- Load sharing: service flow is divided and lead to different member interface according to configured load sharing policy. This is a load sharing on the link level.
- Optimized network management: all the member interfaces in one logical group can be managed at the same time as a normal interface.
- Saving IP addresses: only one IP address is needed for the LAG, and member interfaces do not need IP addresses.

LACP protocol

Link Aggregation Control Protocol (LACP) is based on IEEE802.3ad recommendation. LACP exchanges information with peer through Link Aggregation Control Protocol Data Unit (LACPDU). After enabling LACP of an interface, it notifies the peer of its own LACP priority, system MAC, interface LACP priority, port ID and operation Key by sending LACPDU.

The peer receives LACPDU, compares information with that received by other interfaces, and chooses the interface in Selected status. The interfaces at both ends become consistent in Selected status.

Every member interface in a LAG has an operation Key which indicates the aggregation ability of this interface. The operation Key is created according to the interface configurations (LAG number, speed, duplex mode). Any change of the configurations will lead to recount of the operation Key. In a LAG, all the active interfaces must have the same operation Key.

Interface status

Member interfaces in a LAG have two kinds of statuses:

- Active status: send/receive LACP packets and forward user data. This kind of interfaces is called the working interface.
- Standby status: send/receive LACP packets, but does not forward user data. This kind of interfaces is called the backup interface.

Link aggregation method

There are several methods of link aggregation:

- Manual aggregation mode

This mode is to add several physical interfaces into a LAG, all the Up interfaces make up a logical interface. The link under one logical link can realize load sharing. This mode does not need LACP packet interaction.

- Static LACP aggregation mode

This mode is to negotiate aggregation parameters and select active interfaces by LACP packet. After manually adding several physical interfaces into a LAG, the local device notifies the peer of its own LACP information. The interfaces at both ends elect the active interface, aggregate the link, etc.

- Dynamic LACP aggregation mode

In dynamic LACP aggregation mode, the QSW-8200 series switch creates and deletes the LAG automatically, as well as adding and removing the member interface. Finally it implements link aggregation by using LACP packets. Only when interfaces have the same basic configuration, speed, and duplex mode can they be aggregated into a LAG. In a dynamic LACP LAG, the active interface with the minimum interface number is called the primary interface, and the others are member interfaces.

The main difference between manual aggregation and static/dynamic LACP aggregation is: manual aggregation mode has all the member interfaces in active status and sharing loading flow, while other two LACP aggregation modes have parts of member interfaces in standby status forming standby link.

The QSW-8200 series switch supports manual aggregation and static LACP aggregation modes.

Load sharing

Load sharing mechanism is used in link aggregation. It divides certain service traffic into different links, thus providing a higher performance ability and reliability.

- Load sharing algorithm: choose the output interface of a packet according to different algorithm, including MAC CRC hash mapping and direct mapping
  - Direct-map algorithm: obtain a 3-bit number using XOR of last 3 bits of source MAC and destination MAC, choose output interface based on the 3-bit number (8 different values)
  - CRC algorithm: perform a Hash operation to source MAC and destination MAC first, then perform the XOR operation on the last 3 bit of the two results, and obtain a 3-bit number for choosing output interface.
- Load sharing mode: choose the output interface base on different load sharing mode or their combination. Make sure packets with same attribution sent out from the same interface. By this, the QSW-8200 series switch can achieve a flexible load sharing. You can assign the load sharing based on port ID, ip address, mac in the packet or their combination. There are following modes:
  - SIP: choose the output interface based on the source IP address.
  - DIP: choose the output interface based on the destination IP address.
  - SMAC: choose the output interface based on the source MAC address.
  - DMAC: choose the output interface based on the destination MAC address.
  - SXORDIP: choose the output interface based on the source IP address XOR the destination IP address.
  - SXORDMAC: choose the output interface based on the source MAC address XOR the destination MAC address.
  - SPORTXORSXORDMAC: choose the output interface based on the source interface XOR source MAC address XOR destination MAC address.

The QSW-8200 series switch supports service load sharing based on load sharing mode.

8.1.2 Preparing for configurations

Scenario

Link aggregation can provide higher communication bandwidth and reliability for link between two devices.

It aggregates several physical Ethernet interface together and makes one logical link. This function realizes uplink and downlink flow load sharing among member interfaces and then increases bandwidth; at the same time, the member interfaces dynamically back up each other, which improves link reliability.

Prerequisite

N/A

8.1.3 Default configurations of link aggregation

Default configurations of link aggregation are as below.

Function	Default value
Link aggregation status	Enable
Load balancing mode	Sxordmac mode
Link aggregation group	Existent, in manual mode
LACP system priority	32768
LACP interface priority	32768
LACP interface mode	Active
LACP timeout mode	Slow
Minimum number of active interfaces	1
Maximum number of active interfaces	8

8.1.4 Configuring link aggregation in manual mode

Configure manual link aggregation for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**link-aggregation enable**	Enable link aggregation.
3	Qtech(config)#**link-aggregation loading-sharing mode { dip | dmac | sip | smac | sxordip | sxordmac }**	(Optional) configure load sharing mode for the LAG.

Step	Command	Description
4	Qtech(config)#**interface port-channel** *port-channel-number*	Enter aggregation group configuration mode.
5	Qtech(config-aggregator)#**mode manual** Qtech(config-aggregator)#**exit**	Configure manual link aggregation mode.
6	Qtech(config)#**interface port** *port-list*	Enter physical layer interface configuration mode.
7	Qtech(config-port)#**channel group** *port-channel-number*	Add an interface to the LAG.

Note

In a LAG, member interfaces that share loads must be identically configured. Otherwise, data cannot be forwarded properly. These configurations include STP, QoS, QinQ, VLAN, interface properties, and MAC address learning.

- STP status on the interface, properties (point-to-point/non point-to-point) of the link connected to the interface, path cost of the interface, STP priority, packet Tx speed limit, whether the interface is configured with loopback protection, root protection, and whether the interface is an edge interface.
- QoS: traffic policing, traffic shaping, congestion avoidance, rate limiting, SP queue, WRR queue scheduling, WFQ queue, interface priority, and interface trust mode.
- QinQ: QinQ status on the interface, added outer VLAN tag, policies for adding outer VLAN Tags for different inner VLAN IDs.
- VLAN: the allowed VLAN, default VLAN, and the link type (Trunk, Hybrid, and Access) on the interface, and whether VLAN packets carry Tag.
- Interface properties: speed, duplex mode, and link Up/Down status.
- MAC address learning: MAC address learning status, MAC address limit configuration, and whether continue to forwarding packets after the MAC address entries exceed the threshold.

8.1.5 Configuring static LACP link aggregation

Configure static LACP link aggregation for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**link-aggregation enable**	(Optional) enable link aggregation.
3	Qtech(config)#**link-aggregation loading-sharing mode** { **dip** | **dmac** | **sip** | **smac** | **sxordip** | **sxordmac** }	(Optional) configure LAG loading sharing mode

Step	Command	Description
4	Qtech(config)#**lacp system-priority** *system-priority*	(Optional) configure the system LACP priority. The end with a higher system LACP priority is the active end. LACP selects the active interface and standby interface based on configurations on the active end. The smaller the value is, the higher the system LACP priority is. If the system LACP priorities are identical, select the one with a smaller MAC address as the active end.
5	Qtech(config)#**lacp timeout** { **fast** | **slow** }	(Optional) configure LACP timeout mode.
6	Qtech(config)#**interface port-channel** *port-channel-number*	Enter LAG configuration mode.
7	Qtech(config-aggregator)#**mode lacp-static**	Configure the static LACP LAG.
8	Qtech(config-aggregator)#{ **max-active** | **min-active** } **links** *number* Qtech(config-aggregator)#**exit**	(Optional) configure the maximum or minimum number of active interfaces in the LACP LAG.
9	Qtech(config)#**interface port** *port-list*	Enter physical layer interface configuration mode.
10	Qtech(config-port)#**channel group** *port-channel-number*	Add a member interface into the LACP LAG.
11	Qtech(config-port)#**lacp port-priority** *port-priority*	(Optional) configure interface LACP priority. The priority influents default interface selection for LACP. The smaller the value is, the higher the system LACP priority is.
12	Qtech(config-port)#**lacp mode** { **active** | **passive** }	(Optional) configure LACP mode for member interface. LACP connection will fail when both ends of a link are in passive mode.

Note

The system selects a default interface based on the following conditions in order: whether the neighbour is discovered, maximum interface rate, highest interface LACP priority, and smallest interface number. The default interface is in active status. Interfaces, which have the same interface rate, peer device, and operation key with the default interface, are in active status. Other interfaces are in standby status.

8.1.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Qtech#show lacp internal [ detail ]`	Show local system LACP information.
2	`Qtech#show lacp neighbor[ detail ]`	Show peer LACP information.
3	`Qtech#show lacp statistics [ port-list port-list ]`	Show LACP statistics on the interface.
4	`Qtech#show lacp sys-id`	Show system ID used by LACP.
5	`Qtech#show link-aggregation`	Show link aggregation information.

8.1.7 Maintenance

Maintain the QSW-8200 series switch as below.

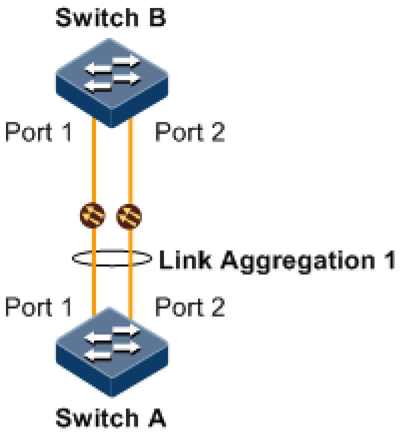
Command	Description
`Qtech(config)#clear lacp statistics [ port-list port-list ]`	Clear statistics of LACP packets.

8.1.8 Example for configuring link aggregation in manual mode

Networking requirements

As shown in Figure 8-2, to improve link reliability between Switch A and Switch B, configure manual link aggregation for the two Switch devices; add port 1 and port 2 into a LAG to build up a unique logical interface. Member interfaces in the LAG share loads according to the source MAC address.

Figure 8-2 Manual link aggregation networking



Configuration steps

Switch B has similar configuration steps as Switch A, so only configurations of Switch A are listed here.

Step 1 Create a manual LAG.

```
Qtech#hostname SwitchA
SwitchA#config
SwitchA(config)#interface port-channel 1
SwitchA(config-aggregator)#mode manual
SwitchA(config-aggregator)#exit
```

Step 2 Add interfaces into the LAG.

```
SwitchA(config)#interface port 1
SwitchA(config-port)#channel group 1
SwitchA(config-port)#exit
SwitchA(config)#interface port 2
SwitchA(config-port)#channel group 1
SwitchA(config-port)#exit
```

Step 3 Configure load sharing mode for link aggregation.

```
SwitchA(config)#link-aggregation load-sharing mode smac
```

Step 4 Enable link aggregation.

```
SwitchA(config)#link-aggregation enable
```

Checking results

Use the **show link-aggregation** to show global configurations of manual link aggregation.

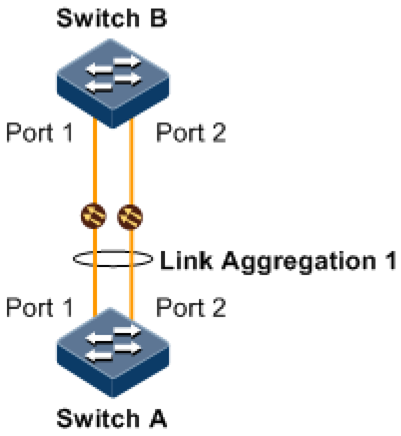
```
SwitchA#show link-aggregation
Link aggregation status:Enable
Load sharing mode:SMAC
Load sharing ticket generation algorithm:Direct-map
  M - Manual  L - Lacp-static
GroupID  Mode  MinLinks  MaxLinks UpLinks Member Port List  Efficient Port
List
-----------------------------------------------------------------
1       M     1        8        2      1-2           1-2
2       M     1        8        0
3       M     1        8        0
```

8.1.9 Example for configuring static LACP link aggregation

Networking requirements

As shown in Figure 8-3, to improve link reliability between Switch A and Switch B, you can configure a static LACP mode link aggregation. That is to add port 1 and port 2 into one LAG; wherein port 1 is used as the active interface and port 2 is the standby interface.

Figure 8-3 Static LACP mode Link aggregation networking



Configuration steps

Step 1 Create static LACP link aggregation

Configure Switch A.

```
Qtech#hostname SwitchA
SwitchA#config
SwitchA(config)#interface port-channel 1
SwitchA(config-aggregator)#mode lacp-static
SwitchA(config-aggregator)#max-active links 1
SwitchA(config-aggregator)#exit
```

Configure Switch B.

```
Qtech#hostname SwitchB
SwitchB#config
SwitchB(config)#interface port-channel 1
SwitchB(config-aggregator)#mode lacp-static
SwitchB(config-aggregator)#exit
```

Step 2 Configure LACP system priority and LACP interface priority, and set Switch A as the active end.

Configure Switch A.

```
SwitchA(config)#lacp system-priority 1000
SwitchA(config)#interface port 1
SwitchA(config-port)#lacp port-priority 1000
```

Step 3 Add interfaces to the LAG

Configure Switch A.

```
SwitchA(config)#interface port 1
SwitchA(config-port)#channel group 1
SwitchA(config-port)#exit
SwitchA(config)#interface port 2
SwitchA(config-port)#channel group 1
SwitchA(config-port)#exit
```

Configure Switch B

```
SwitchB(config)#interface port 1
SwitchB(config-port)#channel group 1
SwitchB(config-port)#exit
SwitchB(config)#interface port 2
SwitchB(config-port)#channel group 1
SwitchB(config-port)#exit
```

Step 4 Enable link aggregation

Configure Switch A.

```
SwitchA(config)#link-aggregation enable
```

Configure Switch B

```
SwitchB(config)#link-aggregation enable
```

Checking results

Use the **show link-aggregation** command to show global configurations of the static LACP mode link aggregation on Switch A.

```
SwitchA#show link-aggregation
Link aggregation status:Enable
Load sharing mode:SXORDMAC
Load sharing ticket generation algorithm:Direct-map
  M - Manual  L - Lacp-static
GroupID  Mode  MinLinks  MaxLinks UpLinks Member Port List
Efficient Port List
----------------------------------------------------------------------
1        L     1       1        2      1-2     1
2        M     1       8         0
3        M     1       8         0
4        M     1       8          0
5        M     1       8          0
6        M     1       8          0
7        M     1       8          0
8        M     1       8          0
```

Use the **show lacp internal** command to show configurations of local LACP protocol interface status, flag, interface priority, administration key, operation key, and interface state on Switch A.

```
SwitchA#show lacp internal
Flags:
  S - Device is requesting Slow LACPDUs  F - Device is requesting Fast
LACPDUs
  A - Device in Active mode           P - Device in Passive mode

Interface State      Flag    Port-Priority   Admin-key  Oper-key  Port-State
----------------------------------------------------------------------------
P1       active     SA     1000            1          1          0x45
P2       standby     SA     32768           1          1         0x45
```

Use the **show lacp neighbor** command to show configurations of LACP protocol interface status, flag, interface priority, administration key, operation key, and interface state of the peer system on Switch A.

8.2 Interface backup

8.2.1 Introduction

In dual uplink networking, Spanning Tree Protocol (STP) is used to block the redundancy link and implement backup. Though STP can meet users' backup requirements, but it fails to meet switching requirements. Though Rapid Spanning Tree Protocol (RSTP) is used, the convergence is on the second level only.

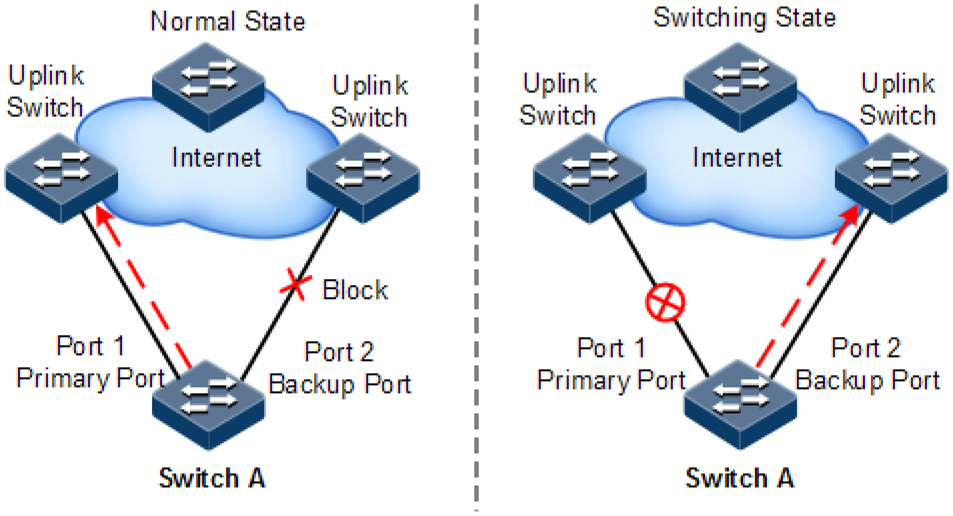
Interface backup, targeted for dual uplink networking, implements backup through primary/backup link. When the primary link fails, traffic is switched to the backup link. In this way, not only 50ms fast switching is ensured, but also configurations are simplified.

Principles

Interface backup is realized by configuring the interface backup group. Each interface backup group contains a primary interface and a backup interface. The link, where the primary interface is, is called a primary link while the link, where the backup interface is, is called the backup interface. Member interfaces in the interface backup group support physical interfaces and LAGs. However, they do not support Layer 3 interfaces.

In the interface backup group, when an interface is in Up status, the other interface is in Standby statue. At any time, only one interface is in Up status. When the Up interface fails, the Standby interface is switched to the Up status.

Figure 8-4 Principles of interface backup



As shown in Figure 8-4, Port 1 and Port 2 on Switch A are connected to their uplink devices respectively. The interface forwarding states are shown as below:

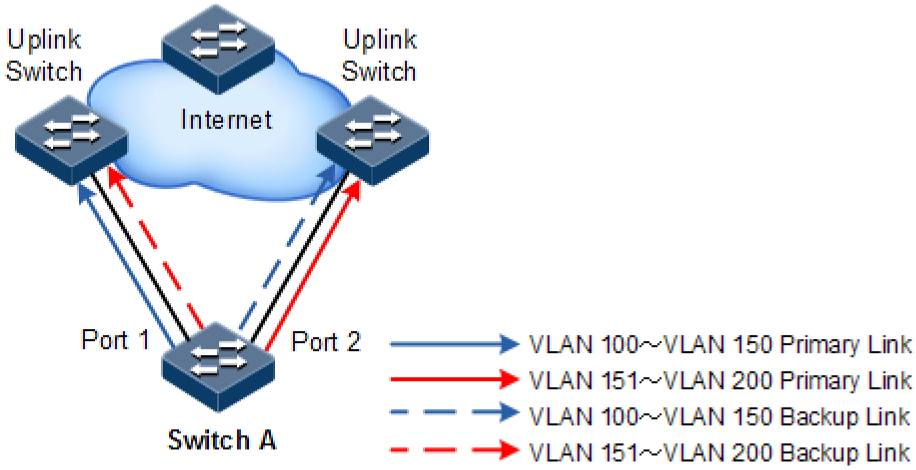
- Under normal conditions, Port 1 is the primary interface while Port 2 is the backup interface. Port 1 and the uplink device forward packet while Port 2 and the uplink device do not forward packets.
- When the link between Port 1 and its uplink device fails, the backup Port 2 and its uplink device forward packets.
- When Port 1 restores normally and keeps Up for a period (restore-delay), Port 1 restores to forward packets and Port 2 restores standby status.

When a switching between the primary interface and the backup interface occurs, the switch sends a Trap to the NMS.

Application of interface backup in different VLANs

By applying interface backup to different VLANs, you can enable two interfaces to share service load in different VLANs, as shown in Figure 8-5.

Figure 8-5 Application of interface backup in different VLANs


Uplink Switch
Internet
Uplink Switch
Port 1
Port 2
Switch A
VLAN 100~VLAN 150 Primary Link
VLAN 151~VLAN 200 Primary Link
VLAN 100~VLAN 150 Backup Link
VLAN 151~VLAN 200 Backup Link

In different VLANs, the forwarding status is shown as below:

- Under normal conditions, configure Switch A in VLANs 100–150.
- In VLANs 100–150, Port 1 is the primary interface and Port 2 is the backup interface.
- In VLANs 151–200, Port 2 is the primary interface and Port 1 is the backup interface.
- In normal situations, Port 1 forwards traffic of VLANs 100–150, and Port 2 forwards traffic of VLANs 151–200.
- When Port 1 or Port 1 link fails, Port 2 forwards traffic of VLANs 100–200.
- When Port 1 restores normally and keeps Up for a period (restore-delay), Port 1 forwards traffic of VLANs 100–150, and Port 2 forwards VLANs 151–200.

8.2.2 Preparing for configurations

Scenario

On a dual uplink network, by configuring interface backup, you can realize backup and fast switching of primary/backup link, and load sharing between different interfaces.

Compared with STP, interface backup not only ensures millisecond level switching, but also simplifies configurations.

Prerequisite

N/A

8.2.3 Default configurations of interface backup

Default configurations of interface backup are listed as below.

Function	Default value
Interface backup group	N/A
Restore-delay	15s
Restoration mode	Interface connection mode (port-up)

8.2.4 Configuring basic functions of interface backup

Caution

Interface backup and STP, loopback detection, Ethernet ring, ELPS, or ERPS may interfere with each other. Configuring two or more of them concurrently on an interface is not recommended.

Configure basic functions of interface backup for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface** *interface-type primary-interface-number*	Enter physical layer interface configuration mode or aggregation group configuration mode.
3	Qtech(config-port)#**switchport backup** *interface-type backup-interface-number* [**vlanlist** *vlan-list*] Qtech(config-port)#**exit**	Configure the interface backup group. If no VLAN list is specified, the VLAN ranges from 1 to 4094.
	Qtech(config-aggregator)#**switchport backup** *interface-type backup-interface-number* **vlanlist** *vlan-list* Qtech(config-aggregator)#**exit**	
4	Qtech(config)#**switchport backup restore-delay** *period*	(Optional) configure the restore-delay period.
5	Qtech(config)#**switchport backup restore-mode** { **disable** | **neighbor-discover** | **port-up** }	(Optional) configure restoration mode.

Note

In a VLAN, an interface or a LAG can be a member of only one interface backup group.

8.2.5 (Optional) configuring FS on interface

Caution

- After Force Switch (FS) is successfully configured, the primary/backup link will be switched; namely, the current link is switched to the backup link (without considering Up/Down status of the primary/backup interface).
- In the FS command, the backup interface number optional. If the primary interface is configured with multiple interface backup groups in corresponding VLANs, you should input the backup interface number.

Configure FS on the interface for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface** *interface-type primary-interface-number*	Enter physical layer interface configuration mode or aggregation group configuration mode.
3	Qtech(config-port)#**switchport backup** *interface-type backup-interface-number* **force-switch**	Configure FS on the interface. You can use the **no switchport backup** [*interface-type backup-interface-number*] **force-switch** command to cancel FS. Then, the principles of selecting the working link according to link status are as below: ● If the Up/Down statuses of the two interfaces are the same, the primary interface is of high priority. ● If the Up/Down statuses of the two interfaces are different, the Up interface is of high priority.
	Qtech(config-aggregator)#**switchport backup** *interface-type backup-interface-number* **force-switch**	

8.2.6 Configuring peer interface backup

Configure peer interface backup for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface** *interface-type primary-interface-number*	Enter physical layer interface configuration mode or aggregation group configuration mode.
3	Qtech(config-port)#**switchport peer-backup vlanlist** *vlan-list* **md** *md-name* **ma** *ma-name* **level** *level* **remote-mep** *mep-id*	Configure the peer interface backup group on the device with the primary interface.

8.2.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show switchport backup**	Show status of interface backup.
2	Qtech#**show switchport peer-backup** [*interface-type interface-list*]	Show configurations of the peer interface backup group.

8.2.8 Example for configuring interface backup

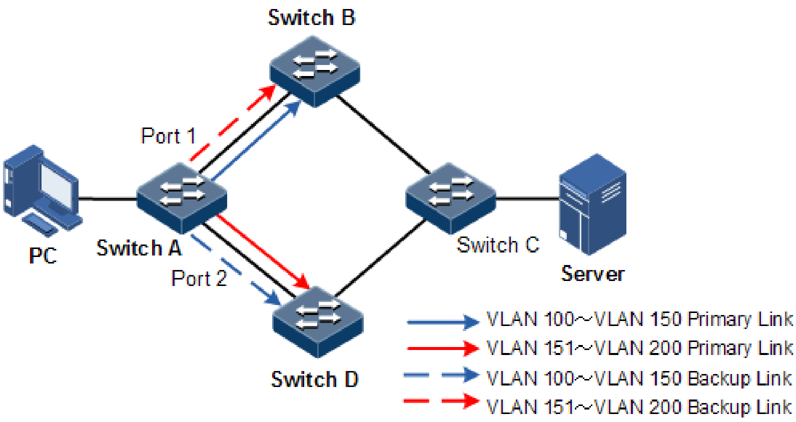
Networking requirements

As shown in Figure 8-6, the PC accesses the server through the Switch. To realize a reliable remote access from the PC to the server, configure an interface backup group on Switch A and specify the VLAN list so that the two interfaces concurrently forward services in different VLANs and share load. Configure Switch A as below:

- Add port 1 to VLANs 100–150 as the primary interface and port 2 as the backup interface.
- Add port 2 to VLANs 151–200 as the primary interface and port 1 as the backup interface.

When port 1 or its link fails, the system switches to the backup interface port 2 to resume the link.

Figure 8-6 Interface backup networking


Switch B
Port 1
PC
Switch A
Port 2
Switch C
Server
Switch D
VLAN 100~VLAN 150 Primary Link
VLAN 151~VLAN 200 Primary Link
VLAN 100~VLAN 150 Backup Link
VLAN 151~VLAN 200 Backup Link

Configuration steps

Step 1 Create VLANs, and add interfaces to the VLANs.

```
Qtech#config
Qtech(config)#create vlan 100-200 active
Qtech(config)#interface port 1
Qtech(config-port)#switchport mode trunk
Qtech(config-port)#switchport trunk allowed vlan 100-200 confirm
Qtech(config-port)#exit
Qtech(config)#interface port-list 2
Qtech(config-port)#switchport mode trunk
Qtech(config-port)#switchport trunk allowed vlan 100-200 confirm
Qtech(config-port)#exit
```

Step 2 Add port 1 to VLANs 100–150 as the primary interface and port 2 as the backup interface.

```
Qtech(config)#interface port-list 1
Qtech(config-port)#switchport backup port 2 vlanlist 100-150
Qtech(config-port)#exit
```

Step 3 Add port 2 to VLANs 151–200 as the primary interface and port 1 as the backup interface.

```
Qtech(config)#interface port-list 2
Qtech(config-port)#switchport backup port 1 vlanlist 151-200
```

Checking results

Use the **show switchport backup** command to show status of interface backup under normal or faulty conditions.

When both port 1 and port 2 are Up, port 1 forwards traffic of VLANs 100–150, and port 2 forwards traffic of VLANs 151–200.

```
Qtech#show switchport backup
Restore delay: 15s.
Restore mode: port-up.
Active Port(State)    Backup Port(State)    Vlanlist
---------------------------------------------------------
P1      (Up)        P2   (Standby)    100-150
P2      (Up)        P1   (Standby)    151-200
```

Manually disconnect the link between Switch A and Switch B to emulate a fault. Then, port 1 becomes Down, and port 2 forwards traffic of VLANs 100–200.

```
Qtech#show switchport backup
Restore delay: 15s
Restore mode: port-up
Active Port(State)   Backup Port(State)   Vlanlist
-----------------------------------------------------------------
P1 (Down)        P2    (Up)             100-150
P2 (Up)         P1    (Down)           151-200
```

When port 1 resumes and keeps Up for 15s (restore-delay), it forwards traffic of VLANs 100–150 while port 2 forwards traffic of VLANs 151–200.

8.3 ELPS (G.8031)

8.3.1 Introduction

Ethernet Linear Protection Switching (ELPS) is an Automatic Protection Switching (APS) protocol based on the ITU-TG.8031 recommendation. It is an end-to-end protection technology used to protect an Ethernet connection.

ELPS deploys protection resources for working resources, such as path and bandwidth, etc. ELPS technology takes a simple, fast, and predictable mode to realize network resource switching, easier for Carrier to plan network more efficiently and learn network active status.

8.3.2 Preparing for configurations

Scenario

Configuring ELPS feature in Ethernet can make Ethernet reliability up to telecommunication level (network self-heal time less than 50ms). It is an end-to-end protection technology used for protecting an Ethernet link.

ELPS supports 1+1 protection switching and 1:1 protection switching modes:

- 1+1 protection switching: each working line is assigned with a protection line. In the protection domain, the source end sends traffic through the working and protection lines while the destination end receives the traffic from one line.
- 1:1 protection switching: each working line is assigned with a protection line. The source end sends traffic through the working/protection line. In general, the source sends traffic through the working line. The protection line is a backup line. When the working line fails, the source end and destination end communicate through APS protocol to switch traffic to the protection line simultaneously.

Based on whether the source end and destination end switch traffic simultaneously, ELPS is divided into unidirectional switching and bidirectional switching:

- Unidirectional switching: when one direction of a line fails, one end can receive the traffic while the other end fails to receive the traffic. The end failing to receive the traffic detects a fault and switches the traffic. And the other end does not detect the fault and switch traffic. Therefore, both ends may receive the traffic through different lines.
- Bidirectional switching: when a line fails, even in one direction, both ends communicate through APS protocol to switch traffic to the protection line. Therefore, both ends receive and send the traffic through the same line.

This QSW-8200 series switch does not distinguish one-way and bidirectional switching until in 1+1 mode; only bidirectional switching is available in 1:1 mode.

ELPS provides two modes for fault detection:

- Detecting fault over physical interface status: to get link fault quickly and switching in time, available to neighbor devices.
- Detecting fault over CC: available to one-way detection or multi-devices crossing detection.

Prerequisite

- Connect interfaces.

- Configure physical parameters to make interfaces Up at the physical layer.
- Create VLANs.
- Add interfaces into VLANs.
- Configure CFP detection among devices (take preparation when adopting CFP detection mode).

8.3.3 Default configurations of ELPS

Default configurations of ELPS are as below.

Function	Default value
Protection group mode	Revertive mode
WTR timer	5min
HOLDOFF timer	0
Reporting ELPS failure information to network management system	Enable
Failure detection method	Physical link

8.3.4 Creating ELPS pair

Enable ELPS pair for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**ethernet line-protection** *line-id* **working** *interface-type interface-number vlan-list* **protection** *interface-type interface-number vlan-list* { **one-plus-one-bi** | **one-plus-one-uni** | **one-to-one** } [**non-revertive**] [**protocol-vlan** *vlan-id*]	Create the ELPS protection line and configure the protection mode. The protection group is in non-revertive mode if you configure the **non-revertive** parameter. • In revertive mode, when the working line recovers from a fault, traffic is switched from the protection line to the working line. • In non-revertive mode, when the working line recovers from a fault, traffic is not switched from the protection line to the working line.
3	Qtech(config)#**ethernet line-protection** *line-id* **name** *string*	(Optional) configure a name for the ELPS protection line.

Step	Command	Description
4	Qtech(config)#**ethernet line-protection** *line-id* **wtr-timer** *wtr-timer*	(Optional) configure the WTR timer. In revertive mode, when the working line recovers from a fault, traffic is not switched to the working line unless the WTR timer times out. By default the WTR time value is set to 5min. **Note** We recommend that WTR timer configurations on both ends keep consistent. Otherwise, we cannot ensure 50ms quick switching.
5	Qtech(config)#**ethernet line-protection** *line-id* **hold-off-timer** *hold-off-timer*	(Optional) configure the HOLDOFF timer. After the HOLDOFF timer is configured, when the working line fails, the system will delay processing the fault. It means that traffic is delayed to be switched to the protection line. This helps prevent frequent switching caused by working line vibration. By default, the HOLDOFF timer value is set to 0. **Note** If the HOLDOFF timer value is over great, it may influence 50ms switching performance. Therefore, we recommend setting the HOLDOFF timer value to 0.
6	Qtech(config)#**ethernet line-protection trap enable**	(Optional) enable ELPS Trap. By default, ELPS Trap is disabled. Use the **ethernet line-protection trap disable** command to disable ELPS Trap.

8.3.5 Configuring ELPS fault detection mode

Configure ELPS fault detection mode for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.

Step	Command	Description
2	Qtech(config)#**ethernet line-protection** *line-id* { **working** | **protection** } **failure-detect physical-link**	Set the fault detection mode of the working line/protection line to **failure-detect physical-link**. By default, the fault detection mode is set to **failure-detect physical-link**.
	Qtech(config)#**ethernet line-protection** *line-id* { **working** | **protection** } **failure-detect cc** [**md** *md-name*] **ma** *ma-name* **level** *level* **mep** *local-mep-id remote-mep-id*	Set the fault detection mode of the working line/protection line to **failure-detect cc**. This fault detection mode cannot take effect unless you finish related configurations on CFM.
	Qtech(config)#**ethernet line-protection** *line-id* { **working** | **protection** } **failure-detect physical-link-or-cc** [**md** *md-name*] **ma** *ma-name* **level** *level* **mep** *local-mep-id remote-mep-id*	Set the fault detection mode of the working line/protection line to **failure-detect physical-link-or-cc**. In this mode, a Trap is reported when a fault is detected on the physical link/CC. This fault detection mode cannot take effect unless you finish related configurations on CFM.

Note

Fault detection modes of the working line and protection line can be different. However, we recommend keeping fault detection mode configurations of the working line and protection line consistent.

8.3.6 (Optional) configuring ELPS control

Configure ELPS control for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**ethernet line-protection** *line-id* **lockout**	Lock protection switching. After this configuration, the traffic is not switched to the protection line even the working line fails.
3	Qtech(config)#**ethernet line-protection** *line-id* **force-switch**	Switch the traffic from the working line to the protection line forcedly.
4	Qtech(config)#**ethernet line-protection** *line-id* **manual-switch**	Switch the traffic from the working line to the protection line manually. Its priority is lower than the one of FS and APS.

Step	Command	Description
5	Qtech(config)#**ethernet line-protection** *line-id* **manual-switch-to-work**	In non-revertive mode, switch the traffic from the protection line to the working line.
6	Qtech(config)#**clear ethernet line-protection** *line-id* **end-to-end command**	Clear end-to-end switching control commands, including **lockout**, **force-switch**, **manual-switch**, and **manual-switch-to-work**.

Note

By default, traffic is automatically switched to the protection line when the working line fails. Therefore, you need to configure ELPS switching control in some special cases.

8.3.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show ethernet line-protection** [*line-id*]	Show protection link configurations.
2	Qtech#**show ethernet line-protection** [*line-id*] **statistics**	Show protection line statistics.
3	Qtech#**show ethernet line-protection** [*line-id*] **aps**	Show APS protocol information.

8.3.8 Maintenance

Maintain the QSW-8200 series switch as below.

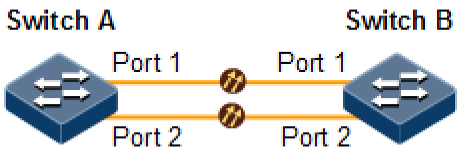
Command	Description
Qtech(config)#**clear ethernet line-protection** [*line-id*] **statistics**	Clear protection line statistic, including Tx APS packets, Rx APS packets, latest switching time, latest status switching time.

8.3.9 Example for configuring 1:1 ELPS protection

Networking requirements

As shown in Figure 8-7, to improve link reliability between Switch A and Switch B, configure 1:1 ELPS on the two Switch devices and detect fault over physical interface status. The port 1 and port 2 belong to VLANs 100–200.

Figure 8-7 1:1 ELPS networking



Configuration steps

Step 1 Create VLANs 100–200 and add interfaces into VLANs 100–200.

Configure Switch A.

```
Qtech#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 100-200 active
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport trunk allowed vlan 100-200 confirm
SwitchA(config-port)#exit
SwitchA(config)#interface port 2
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport trunk allowed vlan 100-200 confirm
SwitchA(config-port)#exit
```

Configure Switch B.

```
Qtech#hostname SwitchB
SwitchB#config
SwitchB(config)#create vlan 100-200 active
SwitchB(config)#interface port 1
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#switchport trunk allowed vlan 100-200 confirm
SwitchB(config-port)#exit
SwitchB(config)#interface port 2
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#switchport trunk allowed vlan 100-200 confirm
SwitchB(config-port)#exit
```

Step 2 Create 1:1 mode ELPS pair.

Configure Switch A.

```
SwitchA(config)#ethernet line-protection 1 working port 1 100-200
protection port 2 100-200 one-to-one
```

Configure Switch B.

```
SwitchB(config)#ethernet line-protection 1 working port 1 100-200
protection port 2 100-200 one-to-one
```

Step 3 Configure fault detection mode.

Configure Switch A.

```
SwitchA(config)#ethernet line-protection 1 working failure-detect
physical-link
SwitchA(config)#ethernet line-protection 1 protection failure-detect
physical-link
```

Configure Switch B.

```
SwitchB(config)#ethernet line-protection 1 working failure-detect
physical-link
SwitchB(config)#ethernet line-protection 1 protection failure-detect
physical-link
```

Checking results

Use the **show ethernet line-protection** command to show configurations of 1:1 ELPS on the QSW-8200 series switch.

Take Switch A for example.

```
SwitchA#show ethernet line-protection 1
Id:1
Name:
ProtocolVlan:100-200
Working(Port-Vlanlist-FaiureDetect-MAID-LocalMep-RemoteMep)(State/LCK):
P1-100-200-physical--0-0-0(Active/N)
Protection(Port-Vlanlist-FaiureDetect-MAID-LocalMep-RemoteMep)(State/F/M):
P2-100-200-physical--0-0-0(Standby/N/N)
Wtr(m):5
Holdoff(100ms):0
```

Use the **show ethernet line-protection aps** command to show configurations of the 1:1 ELPS APS on the QSW-8200 series switch.

Take Switch A for example.

```
SwitchA#show ethernet line-protection 1 aps
Id      Type    Direction Revert Aps State Signal(Requested/Bridged)
```

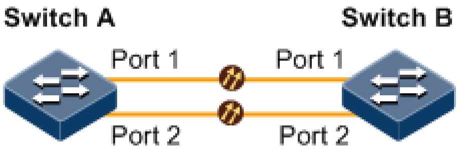
```
------------------------------------------------------------------
1-Local  1:1     bi       yes    yes NR-W  null/null
1-Remote 1:1     bi       yes    yes NR-W  null/null
```

8.3.10 Example for configuring 1+1 ELPS protection pair

Networking requirements

As shown in Figure 8-8, to improve link reliability between Switch A and Switch B, configure 1+1 unidirectional ELPS on the two Switch devices and detect fault over CFM. The port 1 and port 2 belong to VLANs 100–200.

Figure 8-8 1+1 ELPS networking



Configuration steps

Step 1 Create VLANs 100–200, and add interfaces into VLANs 100–200.

Configure Switch A.

```
Qtech#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 100-200 active
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport trunk allowed vlan 100-200 confirm
SwitchA(config-port)#exit
SwitchA(config)#interface port 2
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport trunk allowed vlan 100-200 confirm
SwitchA(config-port)#exit
```

Configure Switch B.

```
Qtech#hostname SwitchB
SwitchB#config
SwitchB(config)#create vlan 100-200 active
SwitchB(config)#interface port 1
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#switchport trunk allowed vlan 100-200 confirm
SwitchB(config-port)#exit
SwitchB(config)#interface port 2
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#switchport trunk allowed vlan 100-200 confirm
SwitchB(config-port)#exit
```

Step 2 Configure CFM.

Configure Switch A.

```
SwitchA(config)#ethernet cfm domain md-name md1 level 7
SwitchA(config)#service ma1 level 7
SwitchA(config-service)#service vlan-list 100
SwitchA(config-service)#service mep down mpid 1 port 1
SwitchA(config-service)#service mep down mpid 2 port 2
SwitchA(config-service)#service remote-mep 3
SwitchA(config-service)#service remote-mep 4
SwitchA(config-service)#service cc enable mep 1
SwitchA(config-service)#service cc enable mep 2
SwitchA(config-service)#exit
SwitchA(config)#ethernet cfm enable
```

Configure Switch B.

```
SwitchB(config)#ethernet cfm domain md-name md1 level 7
SwitchB(config)#service ma1 level 7
SwitchB(config-service)#service vlan-list 100
SwitchB(config-service)#service mep down mpid 3 port 1
SwitchB(config-service)#service mep down mpid 4 port 2
SwitchB(config-service)#service remote-mep 1
SwitchB(config-service)#service remote-mep 2
SwitchB(config-service)#service cc enable mep 3
SwitchB(config-service)#service cc enable mep 4
SwitchB(config-service)#exit
SwitchB(config)#ethernet cfm enable
```

Step 3 Create 1+1 unidirectional ELPS protection line.

Configure Switch A.

```
SwitchA(config)#ethernet line-protection 1 working port 1 100-200
protection port 2 100-200 one-plus-one-uni
```

Configure Switch B.

```
SwitchB(config)#ethernet line-protection 1 working port 1 100-200
protection port 2 100-200 one-plus-one-uni
```

Step 4 Configure fault detection mode.

Configure Switch A.

```
SwitchA(config)#ethernet line-protection 1 working failure-detect cc md
md1 ma ma1 level 7 mep 1 3
SwitchA(config)#ethernet line-protection 1 protection failure-detect cc
md md1 ma ma1 level 7 mep 2 4
```

Configure Switch B.

```
SwitchB(config)#ethernet line-protection 1 working failure-detect cc md
md1 ma ma1 level 7 mep 3 1
SwitchB(config)#ethernet line-protection 1 protection failure-detect cc
md md1 ma ma1 level 7 mep 4 2
```

Checking results

Use the **show ethernet line-protection** command to show configurations of 1+1 ELPS on the QSW-8200 series switch.

Take Switch A for example.

```
SwitchA#show ethernet line-protection 1
Id:1
Name:
ProtocolVlan:100-200
Working(Port-Vlanlist-FaiureDetect-MAID-LocalMep-RemoteMep)(State/LCK):
P1-100-200-cc-md1ma1-7-1-3(Active/N)
Protection(Port-Vlanlist-FaiureDetect-MAID-LocalMep-RemoteMep)(State/F/M):
P2-100-200-cc-md1ma1-7-2-4(Standby/N/N)
Wtr(m):5
Holdoff(100ms):0
```

Use the **show ethernet line-protection aps** command to show 1+1 ELPS APS protocol information on the QSW-8200 series switch.

Take Switch A for example.

```
SwitchA#show ethernet line-protection 1 aps
Id       Type    Direction Revert Aps State Signal(Requested/Bridged)
---------------------------------------------------------------------
1-Local  1+1     uni       yes    yes NR-W  null/normal
```

8.4 ERPS (G.8032)

8.4.1 Introduction

Ethernet Ring Protection Switching (ERPS) is an APS protocol based on the ITU-TG.8032 recommendation. It is a link-layer protocol specially used in Ethernet rings. Generally, ERPS can avoid broadcast storm caused by data loopback in Ethernet rings. When a link/device on the Ethernet ring fails, traffic can be quickly switched to the backup link to ensure restoring services quickly.

ERPS uses the control VLAN in the ring network to transmit ring network control information. Meanwhile, combining with the topology feature of the ring network, it discovers network fault quickly and enable the backup link to restore service fast.

8.4.2 Preparing for configurations

Scenario

With development of Ethernet to Telecom-grade network, voice and video multicast services bring higher requirements on Ethernet redundant protection and fault-recovery time. The fault-recovery time of current STP system is in second level that cannot meet requirements.

By defining different roles for nodes on a ring, ERPS can block a loopback to avoid broadcast storm in normal condition. Therefore, the traffic can be quickly switched to the protection line when working lines or nodes on the ring fail. This helps eliminate the loopback, perform protection switching, and automatically recover from faults. In addition, the switching time is shorter than 50ms.

The QSW-8200 series switch supports the single ring, intersecting ring, and tangent ring.

ERPS provides 2 modes to detect a fault:

- Detect faults based on the physical interface status: learning link fault quickly and switching services immediately, suitable for detecting the fault between neighbor devices.
- Detect faults based on CFM: suitable for unidirectional detection or multi-device crossing detection.

Prerequisite

- Connect interfaces.
- Configure physical parameters to make interfaces Up at the physical layer.
- Create VLANs.
- Add interfaces into VLANs.
- Configure CFP among devices to make them neighbors. (take preparation when adopting CC detection mode).

8.4.3 Default configurations of ERPS

Default configurations of ERPS are as below.

Function	Default value
Protocol VLAN	1

Function	Default value
Protection ring mode	Revertive
Ring WTR timer	5min
Guard timer	500ms
Ring HOLDOFF timer	0ms
ERPS fault information reported to network management system	Disable
Sub-ring virtual circuit mode in crossing node	With
Ring Propagate switch in crossing node	Disable
Fault detection method	Physical interface
WTB timer	5s

8.4.4 Creating ERPS ring

Configure ERPS for the QSW-8200 series switch as below.

⚠ **Caution**

- Only one device on the protection ring can be set to the Ring Protection Link (RPL) Owner and one device is set to RPL Neighbour. Other devices are set to ring forwarding nodes.
- In actual, the tangent ring consists of 2 independent single rings. Configurations on the tangent ring are identical to the ones on the common single ring. The intersecting ring consists of a master ring and a sub-ring. Configurations on the master ring are identical to the ones on the common single ring. For details about configurations on the sub-ring, see section 8.4.5 (Optional) creating ERPS sub-ring.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.

Step	Command	Description
2	Qtech(config)#**ethernet ring-protection** *ring-id* **east** *interface-type interface-number* **west** *interface-type interface-number* [**node-type rpl-owner rpl** { **east** | **west** }] [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create a protection ring and set the node to the RPL Owner. By default, the protocol VLAN is VLAN 1, and the range of blocked VLANs is 1–4094. The protection ring is in non-revertive mode if you configure the **non-revertive** parameter. ● In revertive mode, when the working line recovers from a fault, traffic is switched from the protection line to the working line. ● In non-revertive mode, when the working line recovers from a fault, traffic is not switched from the protection line to the working line. By default, the protection ring is in revertive mode. **Note** The east and west interfaces cannot be the same one.
	Qtech(config)#**ethernet ring-protection** *ring-id* **east** *interface-type interface-number* **west** *interface-type interface-number* **node-type rpl-neighbour rpl** { **east**| **west** } [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create a protection ring, and set the node to the RPL Neighbour.
	Qtech(config)#**ethernet ring-protection** *ring-id* **east** *interface-type interface-number* **west** *interface-type interface-number* [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create a protection line, and set the node to the protection forwarding node.
3	Qtech(config)#**ethernet ring-protection** *ring-id* **name** *string*	(Optional) configure a name for the protection ring. Up to 32 bytes are available.

Step	Command	Description
4	`Qtech(config)#`**`ethernet ring-protection`** *`ring-id`* **`version`** `{` **`1`** `|` **`2`** `}`	(Optional) configure the protocol version. The protocol version of all nodes on a protection ring should be identical. In protocol version 1 protection rings are distinguished based on the protocol VLAN. Therefore, you need to configure different protocol VLANs for protection rings. We recommend configuring different protocol VLANs for protection rings even if protocol version 2 is used. By default, protocol version 1 is used.
5	`Qtech(config)#`**`ethernet ring-protection`** *`ring-id`* **`guard-time`** *`guard-time`*	(Optional) after the ring Guard timer is configured, the failed node does not process APS packets during a period. In a bigger ring network, if the failed node recovers from a fault immediately, it may receive the fault notification sent by the neighbour node on the protection ring. Therefore, the node is in Down status again. You can configure the ring Guard timer to resolve this problem.
6	`Qtech(config)#`**`ethernet ring-protection`** *`ring-id`* **`wtr-time`** *`wtr-time`*	(Optional) configure the ring WTR timer. In revertive mode, when the working line recovers from a fault, traffic is not switched to the working line unless the WTR timer times out. By default, the ring WTR time value is set to 5min.
7	`Qtech(config)#`**`ethernet ring-protection`** *`ring-id`* **`holdeoff-time`** *`holdoff-time`*	(Optional) configure the ring HOLDOFF timer. After the HOLDOFF timer is configured, when the working line fails, the system will delay processing the fault. It means that traffic is delayed to be switched to the protection line. This helps prevent frequent switching caused by working line vibration. By default, the HOLDOFF time is 0. **Note** If the ring HOLDOFF timer value is over great, it may influence 50ms switching performance. Therefore, we recommend setting the ring HOLDOFF timer value to 0.

Step	Command	Description
8	Qtech(config)#**ethernet ring-protection trap enable**	(Optional) enable ERPS Trap. By default, ERPS Trap is disabled. Use the **ethernet ring-protection trap disable** command to disable this function.

8.4.5 (Optional) creating ERPS sub-ring

Caution

- Only the intersecting ring consists of a master ring and a sub-ring.
- Configurations on the master ring are identical to the ones on the single ring/tangent ring. For details, see section 8.4.4 Creating ERPS ring.
- Configurations of non-intersecting nodes of the intersecting ring are identical to the ones on the single ring/tangent ring. For details, see section 8.4.4 Creating ERPS ring.

Configure ERPS crossover rings for QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**ethernet ring-protection** *ring-id* { **east** | **west** } *interface-type interface-number* **node-type rpl-owner** [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create the sub-ring on the intersecting node and set the intersecting node to the RPL Owner. By default, the protocol VLAN is VLAN 1, and the range of blocked VLANs is 1–4094. The protection ring is in non-revertive mode if you configure the **non-revertive** parameter. • In revertive mode, when the working line recovers from a fault, traffic is switched from the protection line to the working line. • In non-revertive mode, when the working line recovers from a fault, traffic is not switched from the protection line to the working line. By default, the protection ring is in revertive mode. **Note** The links between 2 intersecting nodes belong to the master ring. Therefore, when you configure the sub-ring on the intersecting node, you can only configure the west or east interface.

Step	Command	Description
	Qtech(config)#**ethernet ring-protection** *ring-id* { **east** | **west** } *interface-type interface-number* **node-type rpl-neighbour** [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create the sub-ring on the intersecting node and set the intersecting node to the RPL Neighbour.
	Qtech(config)#**ethernet ring-protection** *ring-id* { **east** | **west** } *interface-type interface-number* [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create the sub-ring on the intersecting node and set the intersecting node to the protection forwarding node.
3	Qtech(config)#**ethernet ring-protection** *ring-id* **raps-vc** { **with** | **without** }	(Optional) configure the sub-ring virtual circuit mode on the intersecting node. Because the intersecting node belongs to the master ring, transmission modes of protocol packets in the sub-ring are different from the ones of the master ring. In the sub-ring, transmission modes are divided into **with** and **without** modes. • with: the primary ring provides access for sub-ring APS packets; the sub-ring cross node transmits sub-ring APS packets to the primary ring to use the primary ring to complete communications among sub-ring cross nodes. • without: the sub-ring APS packets on cross nodes need to be ended and cannot be transmitted to the primary ring. This mode requires sub-ring not to block the sub-ring protocol VLAN (to ensure sub-ring packets to pass through Owner), so the sub-ring protocol VLAN cannot be in the sub-ring service VLAN list. By default, the sub-ring virtual circuit adopts the **with** mode. Transmission modes on 2 intersecting nodes must be identical.

Step	Command	Description
4	`Qtech(config)#ethernet ring-protection ring-id propagate enable`	Enable the ring Propagate switch on the intersecting node. Because data of the sub-ring needs to be transmitted through the master ring, there is a MAC address table of the sub-ring on the master ring. When the sub-ring fails, it needs to use the Propagate switch to inform the master ring of refreshing the MAC address table to avoid traffic loss. By default, the Propagate switch is disabled. Use the **ethernet ring-protection** *ring-id* **propagate disable** command to disable this function.

8.4.6 Configuring ERPS fault detection mode

Configure ERPS fault detection mode for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#ethernet ring-protection ring-id { east | west } failure-detect physical-link`	Set the ERPS fault detection mode to physical-link. By default, it is physical-link.
	`Qtech(config)#ethernet ring-protection ring-id { east | west } failure-detect cc [ md md-name ] ma ma-name level level mep local-mep-id remote-mep-id`	Set the ERPS fault detection mode to failure-detect cc. This ERPL fault detection mode cannot take effect unless you finish related configurations on CFM. If you configure the MD, the MA should be below the configured md-level.
	`Qtech(config)#ethernet ring-protection ring-id { east | west } failure-detect physical-link-or-cc [ md md-name ] ma ma-name level level mep local-mep-id remote-mep-id`	Set the ERPS fault detection mode to failure-detect physical-link-or-cc. In this mode, a Trap is reported when a fault is detected on the physical link/CC. This ERPL fault detection mode cannot take effect unless you finish related configurations on CFM. If you configure the MD, the MA should be below the configured md-level.

8.4.7 (Optional) configuring ERPS switching control

Configure ERPS switching control for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**ethernet ring-protection** *ring-id* **force-switch** { **east** | **west** }	Switch the traffic on the protection ring to the west/east interface forcedly.
3	Qtech(config)#**ethernet ring-protection** *ring-id* **manual-switch** { **east** | **west** }	Switch the traffic on the protection ring to the west/east interface manually. Its priority is lower than the one of FS and APS.
4	Qtech(config)#**ethernet ring-protection** *ring-id* **wtb-time** *wtb-time*	This configuration is used on the RPL Owner. After the WTB timer is configured in revertive mode, delay to block the RPL interface when the manual command is cleared, avoiding repeatedly blocking the RPL interface when there are multiple FSs or MSs. By default, it is 5s.
4	Qtech(config)#**clear ethernet ring-protection** *ring-id* { **command** | **statistics** }	Clear switching control commands, including force-switch, manual-switch, WTR timer, and WTB timer.

Note

By default, traffic is automatically switched to the protection line when the working line fails. Therefore, you need to configure ERPS control in some special cases.

8.4.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show ethernet ring-protection**	Show configurations of the ERPS ring.
2	Qtech#**show ethernet ring-protection status**	Show ERPS ring status.
3	Qtech#**show ethernet ring-protection statistics**	Show ERPS statistics.

8.4.9 Maintenance

Maintain the QSW-8200 series switch as below.

Command	Description
Qtech(config)#**clear ethernet ring-protection** *ring-id* **statistics**	Clear protection ring statistics, including latest bridge state switch time, bridge state switch times, number of Tx APS packets, number of Rx APS packets, service flow switch times, etc.
Qtech(config)#**clear ethernet ring** *ring-id* **statistics**	Clear statistics of ring interfaces, including the Ethernet ring ID, ring interface ID, and Hello, Change, Flush, etc. packets.

8.4.10 Example for configuring single ring ERPS

Networking requirements

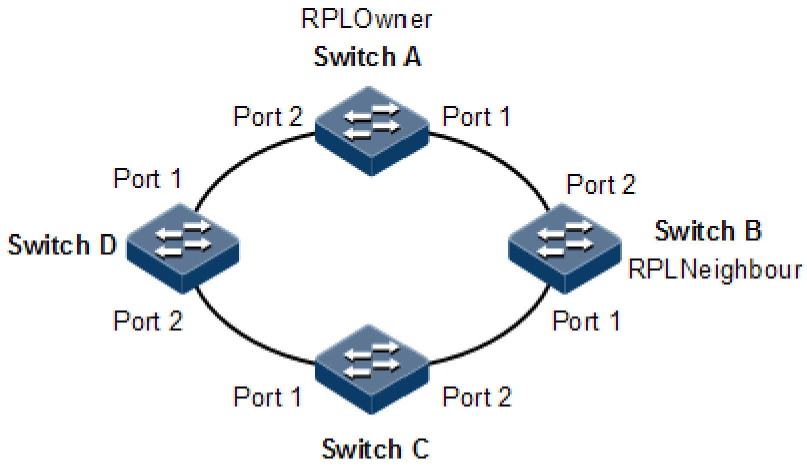
As show in Figure 8-9, to improve Ethernet reliability, the four devices Switch A, Switch B, Switch C, and Switch D build up an ERPS single ring.

Switch A is the RPL Owner, Switch B is the RPL Neighbour, and the RPL link between Switch A and Switch B is blocked.

The fault detection mode between Switch A and Switch D is physical-link-or-cc, other links adopt default fault detection mode (physical-link).

By default, the protocol VLAN is VLAN 1, and the blocked VLANs are VLANs 1–4094.

Figure 8-9 Single ring ERPS networking



Configuration steps

Step 1 Add interfaces into VLANs 1–4094.

Configure Switch A.

```
Qtech#hostname SwitchA
SwitchA#config
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#exit
SwitchA(config)#interface port 2
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#exit
```

Configure Switch B.

```
Qtech#hostname SwitchB
SwitchB#config
SwitchB(config)#interface port 1
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#exit
SwitchB(config)#interface port 2
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#exit
```

Configure Switch C.

```
Qtech#hostname SwitchC
SwitchC#config
SwitchC(config)#interface port 1
SwitchC(config-port)#switchport mode trunk
SwitchC(config-port)#exit
SwitchC(config)#interface port 2
SwitchC(config-port)#switchport mode trunk
SwitchC(config-port)#exit
```

Configure Switch D.

```
Qtech#hostname SwitchD
SwitchD#config
SwitchD(config)#interface port 1
SwitchD(config-port)#switchport mode trunk
SwitchD(config-port)#exit
SwitchD(config)#interface port 2
SwitchD(config-port)#switchport mode trunk
SwitchD(config-port)#exit
```

Step 2 Configure CFM.

Configure Switch A.

```
SwitchA(config)#ethernet cfm domain md-name md1 level 7
SwitchA(config)#service ma1 level 7
SwitchA(config-service)#service vlan-list 1
SwitchA(config-service)#service mep down mpid 1 port 2
SwitchA(config-service)#service remote-mep 2
SwitchA(config-service)#service cc enable mep 1
SwitchA(config-service)#exit
SwitchA(config)#ethernet cfm enable
```

Configure Switch D.

```
SwitchD(config)#ethernet cfm domain md-name md1 level 7
SwitchD(config)#service ma1 level 7
SwitchD(config-service)#service vlan-list 1
SwitchD(config-service)#service mep down mpid 2 port 1
SwitchD(config-service)#service remote-mep 1
SwitchD(config-service)#service cc enable mep 2
SwitchD(config-service)#exit
SwitchD(config)#ethernet cfm enable
```

Step 3 Create an ERPS protection ring.

Configure Switch A.

```
SwitchA(config)#ethernet ring-protection 1 east port 1 west port 2 node-
type rpl-owner rpl east
```

Configure Switch B.

```
SwitchB(config)#ethernet ring-protection 1 east port 1 west port 2 node-
type rpl-neighbour rpl west
```

Configure Switch C.

```
SwitchC(config)#ethernet ring-protection 1 east port 1 west port 2
```

Configure Switch D.

```
SwitchD(config)#ethernet ring-protection 1 east port 1 west port 2
```

Step 4 Configure fault detection mode.

Configure Switch A.

```
SwitchA(config)#ethernet ring-protection 1 west failure-detect physical-
link-or-cc md md1 ma ma1 level 7 mep 1 2
```

Configure Switch D.

```
SwitchD(config)#ethernet ring-protection 1 east failure-detect physical-
link-or-cc md md1 ma ma1 level 7 mep 2 1
```

Checking results

Use the **show ethernet ring-protection status** command to check whether the ERPS protection ring has taken effect on the QSW-8200 series switch.

Take Switch A for example, RPL link is blocked to avoid loopback.

```
SwitchA#show ethernet ring-protection status
Id/Name  Status   Last Occur(ago)   East-State West-State sc Traffic-
vlanlist
---------------------------------------------------------------------
1       idle   0 day 0:0:50:750   block      forwarding  1  1-4094
```

Manually disconnect the link between Switch B and Switch C to simulate a fault, use the following command to show ERPS protection ring status on Switch A again. The RPL link switches to forwarding status.

```
SwitchA#show ethernet ring-protection status
Id/Name  Status   Last Occur(ago)   East-State West-State sc Traffic-
vlanlist
-------------------------------------------------------------------
1      Protection  0 day 0:0:55:950  forwarding forwarding  2  1-4094
```

8.4.11 Example for configuring intersecting G.8032

Networking requirements

As shown in Figure 8-10, to improve Ethernet reliability, Switch A, Switch B, Switch C, Switch D, Switch E and Switch F build up an intersecting G.8032 network.

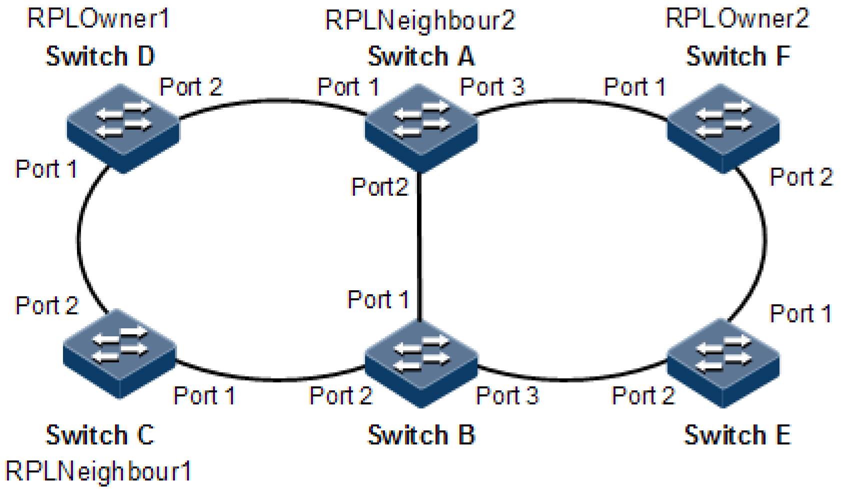
- Switch A, Switch B, Switch C and Switch D build up the master ring, Switch D is master ring RPL Owner, Switch C is master ring RPL Neighbour, block Port 1 Switch D, protocol VLAN is default value 1.

- Switch A, Switch B, Switch E, and Switch F form a sub-ring, Switch F is secondary ring RPL Owner, Switch A is sub-ring RPL Neighbour, congest Switch F Port 1, protocol VLAN is 4094. Virtual path mode of sub-ring is defaulted with mode.

The range of blocked VLANs for the master ring and sub-ring is defaulted to VLANs 1–4094.

Devices on the master ring adopt physical-link-or-cc fault detection mode while devices on the sub-ring adopt the default fault detection mode (physical-link).

Figure 8-10 Intersecting ring G.8032 networking



Configuration steps

Step 1 Create VLAN 4094, and add interfaces into VLANs 1–4094.

Configure Switch A.

```
Qtech#hostname SwitchA
SwitchA#config
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#exit
SwitchA(config)#interface port 2
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#exit
SwitchA(config)#interface port 3
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#exit
```

Configure Switch B.

```
Qtech#hostname SwitchB
SwitchB#config
SwitchB(config)#interface port 1
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#exit
SwitchB(config)#interface port 2
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#exit
SwitchB(config)#interface port 3
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#exit
```

Configure Switch C.

```
Qtech#hostname SwitchC
SwitchC#config
SwitchC(config)#interface port 1
SwitchC(config-port)#switchport mode trunk
SwitchC(config-port)#exit
SwitchC(config)#interface port 2
SwitchC(config-port)#switchport mode trunk
SwitchC(config-port)#exit
```

Configure Switch D.

```
Qtech#hostname SwitchD
SwitchD#config
SwitchD(config)#interface port 1
SwitchD(config-port)#switchport mode trunk
SwitchD(config-port)#exit
SwitchD(config)#interface port 2
SwitchD(config-port)#switchport mode trunk
SwitchD(config-port)#exit
```

Configure Switch E.

```
Qtech#hostname SwitchE
SwitchE#config
SwitchE(config)#interface port 1
SwitchE(config-port)#switchport mode trunk
SwitchE(config-port)#exit
SwitchE(config)#interface port 2
SwitchE(config-port)#switchport mode trunk
SwitchE(config-port)#exit
```

Configure Switch F.

```
Qtech#hostname SwitchF
SwitchF#config
```

```
SwitchF(config)#interface port 1
SwitchF(config-port)#switchport mode trunk
SwitchF(config-port)#exit
SwitchF(config)#interface port 2
SwitchF(config-port)#switchport mode trunk
SwitchF(config-port)#exit
```

Step 2 Configure CFM detection on the master ring.

Configure Switch A.

```
SwitchA(config)#ethernet cfm domain md-name md1 level 7
SwitchA(config)#service ma1 level 7
SwitchA(config-service)#service vlan-list 1
SwitchA(config-service)#service mep down mpid 1 port 1
SwitchA(config-service)#service mep down mpid 2 port 2
SwitchA(config-service)#service cc enable mep 1
SwitchA(config-service)#service cc enable mep 2
SwitchA(config-service)#exit
SwitchA(config)#ethernet cfm enable
```

Configure Switch B.

```
SwitchB(config)#ethernet cfm domain md-name md1 level 7
SwitchB(config)#service ma1 level 7
SwitchB(config-service)#service vlan-list 1
SwitchB(config-service)#service mep down mpid 3 port 1
SwitchB(config-service)#service mep down mpid 4 port 2
SwitchB(config-service)#service cc enable mep 3
SwitchB(config-service)#service cc enable mep 4
SwitchB(config-service)#exit
SwitchB(config)#ethernet cfm enable
```

Configure Switch C.

```
SwitchC(config)#ethernet cfm domain md-name md1 level 7
SwitchC(config)#service ma1 level 7
SwitchC(config-service)#service vlan-list 1
SwitchC(config-service)#service mep down mpid 5 port 1
SwitchC(config-service)#service mep down mpid 6 port 2
SwitchC(config-service)#service cc enable mep 5
SwitchC(config-service)#service cc enable mep 6
SwitchC(config-service)#exit
SwitchC(config)#ethernet cfm enable
```

Configure Switch D.

```
SwitchD(config)#ethernet cfm domain md-name md1 level 7
SwitchD(config)#service ma1 level 7
SwitchD(config-service)#service vlan-list 1
SwitchD(config-service)#service mep down mpid 7 port 1
SwitchD(config-service)#service mep down mpid 8 port 2
SwitchD(config-service)#service cc enable mep 7
SwitchD(config-service)#service cc enable mep 8
SwitchD(config-service)#exit
SwitchD(config)#ethernet cfm enable
```

Step 3 Create the master ring of ERPS protection.

Configure Switch A.

```
SwitchA(config)#ethernet ring-protection 1 east port 1 west port 2
```

Configure Switch B.

```
SwitchB(config)#ethernet ring-protection 1 east port 1 west port 2
```

Configure Switch C.

```
SwitchC(config)#ethernet ring-protection 1 east port 1 west port 2 node-
type rpl-neighbour rpl west
```

Configure Switch D.

```
SwitchD(config)#ethernet ring-protection 1 east port 1 west port 2 node-
type rpl-owner rpl east
```

Step 4 Configure fault detection mode on the master ring.

Configure Switch A.

```
SwitchA(config)#ethernet ring-protection 1 east failure-detect physical-
link-or-cc md md1 ma ma1 level 7 mep 1 8
SwitchA(config)#ethernet ring-protection 1 west failure-detect physical-
link-or-cc md md1 ma ma1 level 7 mep 2 3
```

Configure Switch B.

```
SwitchB(config)#ethernet ring-protection 1 east failure-detect physical-
link-or-cc md md1 ma ma1 level 7 mep 3 2
SwitchB(config)#ethernet ring-protection 1 west failure-detect physical-
link-or-cc md md1 ma ma1 level 7 mep 4 5
```

Configure Switch C.

```
SwitchC(config)#ethernet ring-protection 1 east failure-detect physical-
link-or-cc md md1 ma ma1 level 7 mep 5 4
SwitchC(config)#ethernet ring-protection 1 west failure-detect physical-
link-or-cc md md1 ma ma1 level 7 mep 6 7
```

Configure Switch D.

```
SwitchD(config)#ethernet ring-protection 1 east failure-detect physical-
link-or-cc md md1 ma ma1 level 7 mep 7 6
SwitchD(config)#ethernet ring-protection 1 west failure-detect physical-
link-or-cc md md1 ma ma1 level 7 mep 8 1
```

Step 5 Configure the sub-ring of ERPS protection.

Configure Switch A.

```
SwitchA(config)#ethernet ring-protection 2 east port 3 node-type rpl-
neighbour protocol-vlan 4094
SwitchA(config)#ethernet ring-protection 2 propagate enable
```

Configure Switch B.

```
SwitchB(config)#ethernet ring-protection 2 east port 3 protocol-vlan 4094
SwitchB(config)#ethernet ring-protection 2 propagate enable
```

Configure Switch E.

```
SwitchE(config)#ethernet ring-protection 2 east port 1 west port 2
protocol-vlan 4094
```

Configure Switch F.

```
SwitchF(config)#ethernet ring-protection 2 east port 1 west port 2 node-
type rpl-owner rpl east protocol-vlan 4094
```

Checking results

Use the **show ethernet ring-protection status** command to show configurations of the G.8032 protection ring on the QSW-8200 series switch.

Use the command on Switch A, Switch D and Switch F respectively. The result should be as below after the WTR timer expires.

```
SwitchA#show ethernet ring-protection status
Id/Name  Status   Last Occur(ago)East-State West-State sc   Traffic-
vlanlist
------------------------------------------------------------------------
1       idle   0 day 0:0:50:750   forwarding  forwarding 1     1-4094
------------------------------------------------------------------------
2       idle   0 day 0:0:50:750   forwarding  forwarding 1     1-4094

SwitchD#show ethernet ring-protection status
Id/Name  Status   Last Occur(ago)   East-State West-State sc Traffic-
vlanlist
------------------------------------------------------------------------
1       idle   0 day 0:0:50:750   block      forwarding   1   1-4094

SwitchF#show ethernet ring-protection status
Id/Name  Status   Last Occur(ago)   East-State West-State sc Traffic-
vlanlist
------------------------------------------------------------------------
2       idle   0 day 0:0:50:750   block      forwarding   1   1-4094
```

8.5 Failover

8.5.1 Introduction

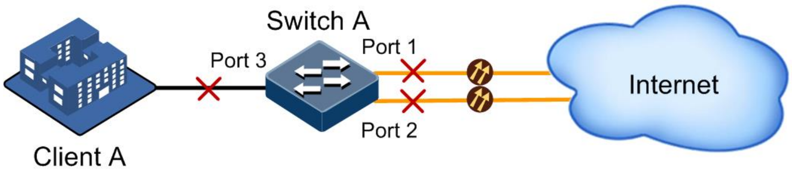
Failover provides an interface linkage scheme to expand the range of link backup. By monitoring the uplinks and synchronizing downlinks, the fault generated on the uplink device can be transmitted to downlink devices to trigger switching. This helps avoid traffic loss when downlink devices cannot sense faults of uplinks.

A fault source is preconfigured when the user creates failover group. A fault source corresponds to a failover group. The fault source includes the interface list, RMEP, and G.8031 switchover.

When a fault source encounters fault, the fault pass group can execute the following actions: shut down interface, send Trap packets, delete a VLAN, suspend a VLAN, modify interface PVID, clear G.8032 ring MAC address, clear Ethernet ring MAC address, etc. The failover group can take only one action over a fault source.

When the fault source is an interface list, failover occurs only when all fault source interfaces are faulty. As shown in Figure 8-11, the uplink interfaces port 1 and port 2 and downlink interface port 3 are added to a failover group. When all the uplink interfaces are faulty, the downlink interface is set Down. If one uplink interface resumes, the downlink interface resumes Up so that it informs downstream devices of the uplink status in time. The fault of the downlink interface does not affect the uplink interface.

Figure 8-11 Failover based on interface



8.5.2 Preparing for configurations

Scenario

When an uplink device on the intermediate device has fault, traffic cannot switch to the protection line if it cannot notify the downlink device in time, and then traffic will be interrupted.

Failover can trigger a preconfigured action upon fault so that the fault status of an upstream device is quickly delivered to the downstream device and master/slave switchover is triggered.

Prerequisite

- Connect interfaces.
- Configure physical parameters to make interfaces Up at the physical layer.

8.5.3 Default configurations of failover

Default configurations of failover are listed below.

Function	Default value
Failover group	N/A
Fault processing action	Shutdown

8.5.4 Creating failover group

Creating failover group based on interface

Create a failover group based on interface for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.

Step	Command	Description
2	Qtech(config)#**link-state-tracking group** *group-number*	Create a failover group, and enable failover.
3	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
4	Qtech(config-port)#**link-state-tracking group** *group-number* { **downstream** | **upstream** }	Configure the failover group and interface type for the interface. An interface belongs to only one group, and can be either an uplink interface or a downlink interface.

Note

- A failover group can contain several uplink interfaces. Failover will not occur when at least one uplink interface is Up. Only when all uplink interfaces are Down can failover occur.
- In global configuration mode, if you use the **no link-state-tracking group** *group-number* command to disable failover, the group will be deleted.
- Use the **no link-state-tracking group** command to delete an interface from failover group in physical layer interface mode. If there is no other interface and the failover group is disabled, the failover group will be deleted when the interface is deleted.

Creating failover group based on RMEP

Create a failover group based on RMEP for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**link-state-tracking group** *group-number* **upstream cfm-mepid** *mep-id* [**ma-name** *name*]	Create a failover group based on RMEP, and enable failover.

Creating failover group based on ELPS

Create a failover group based on ELPS for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**link-state-tracking group** *group-number* **upstream elps-8031-link** *value*	Create a failover group based on ELPS, and enable failover.

Caution

When you create a failover group based on ELPS and configure the downlink action to shut down the interface list, you must ensure that these interfaces are not related to ELPS.

Creating failover group based on link aggregation

Create a failover group based on link aggregation for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**link-state-tracking group** *group-number* **upstream link-aggregation** *link-number*	Create a failover group based on link aggregation, and enable failover.

Creating failover group based on interface backup

Create a failover group based on interface backup for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**link-state-tracking group** *group-number* **upstream port-backup** { **port** | **port-channel** } *pri-interface-number* { **port** | **port-channel** } *backup-interface-number*	Create a failover group based on interface backup, and enable failover.

Creating failover group based on clearing MAC information

Create a failover group based on clearing MAC information about the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**link-state-tracking group** *group-number* **upstream flush-mac-signal**	Create a failover group based on clearing MAC information, and enable failover.

8.5.5 Configuring action taken for downlink interface fault

Configure the action taken for downlink interface fault for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**link-state-tracking group** *group-number* **action** { **delete-vlan** *vlan-id* | **modify-pvid** *vlan-id* | **suspend-vlan** *vlan-id* | **flush-g8032** *rind-id* |**send-flush-mac-signal** }	Enable action taken for clearing faults on the failover interface.

8.5.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show link-state-tracking group** [*group-number*]	Show failover group configurations and status.

9 OAM

This chapter describes basic principles and configurations of OAM, and provides related configuration examples, including the following sections:

- EFM (IEEE 802.3ah)
- CFM (IEEE 802.1ag/ITU-Y.1731)
- SLA
- Service

9.1 EFM (IEEE 802.3ah)

9.1.1 Introduction

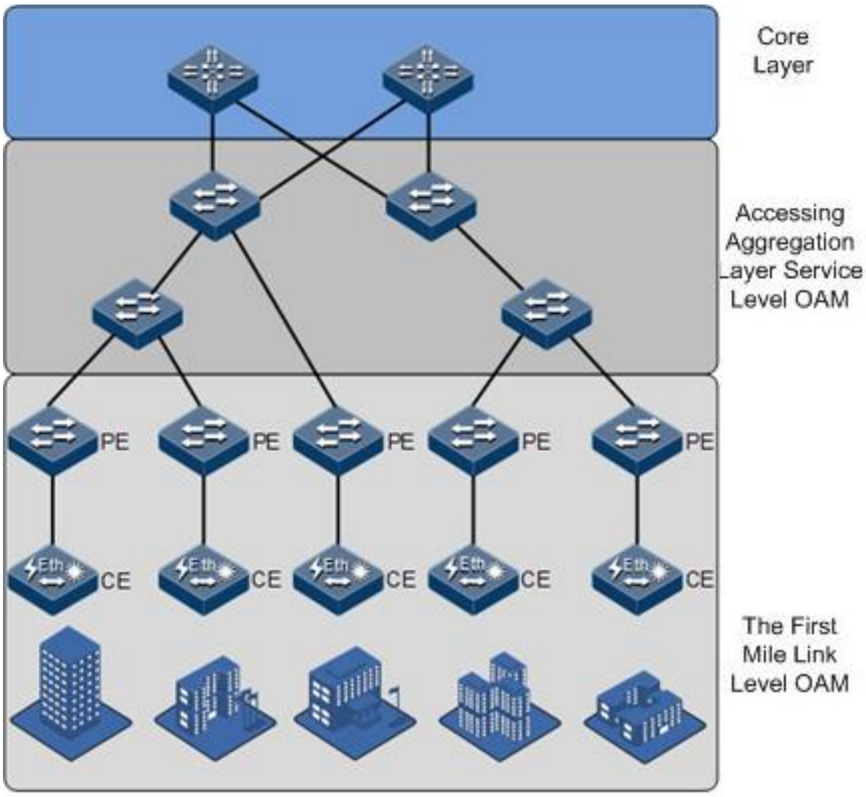
Initially, Ethernet is designed for LANs. Operation, Administration and Maintenance (OAM) is weak in performance because of its small size and NE-level administrative system. With continuous development of Ethernet technology, the application scale of Ethernet in carrier-grade network becomes wider and wider. Compared with LAN, Compared with LAN, the carrier-grade network requires a much longer link length and bigger size. Lack of an effective management and maintenance mechanism has become the biggest obstacle for the Ethernet to be applied on the carrier-grade network.

To confirm connectivity of Ethernet virtual connection, effectively detect faults, confirm, and locate faults on Ethernet layer, balance network utilization, measure network performance, and provide service according to Service Level Agreement (SLA), implementing OAM is a must for widespread use of the carrier-grade Ethernet.

Ethernet OAM is realized in different levels, as shown in Figure 9-1, and there are two levels:

- Link-level Ethernet OAM: it is applied in Ethernet physical link (that is the first mile) between Provider Edge (PE) and Customer Edge (CE), which is used to monitor link state between the user network and carrier network, and the typical protocol is Ethernet in the First Mile (EFM) OAM protocol.
- Service-level Ethernet OAM: it is applied at access aggregation layer of network, which is used to monitor connectivity of the entire network, locate connectivity fault of network, monitor and control performance of links, The typical protocol is Connectivity Fault Management (CFM) OAM protocol.

Figure 9-1 OAM classification


Core Layer
Accessing Aggregation Layer Service Level OAM
PE
PE
PE
PE
PE
Eth
CE
CE
CE
CE
CE
The First Mile Link Level OAM

Compliant with the IEEE 802.3ah protocol, Ethernet in the First Mile (EFM) is a link-level Ethernet OAM technology. It provides link connectivity detection, link fault monitoring, and remote fault notification, etc. for a link between two directly connected devices.

"The first mile" in EFM is the connection between a local device of the carrier and a client device. The target is that Ethernet technology will be extended to access network market of telecom users, to improve network performance, and reduce cost on the device and operation. EFM is used in Ethernet link of user access network edge.

The QSW-8200 series switch provides EFM with IEEE 802.3ah standard.

9.1.2 Preparing for configurations

Scenario

Deploying EFM feature between directly connected devices can efficiently improve Ethernet link management and maintenance capability and ensure stable network operation.

Prerequisite

- Connect interfaces.
- Configure physical parameters to make interfaces Up at the physical layer.

9.1.3 Default configurations of EFM

Default configurations of EFM are as below.

Function	Default value
EFM working mode	Passive
Interval for sending packets	10×100ms
Link timeout time	5s
OAM status	Disable
Peer OAM event alarm status	Disable
EFM remote loopback state	No response
Monitor window of errored frame event	1s
Monitor threshold of error event	1 errored frame
Monitor window of errored frame period event	1000ms
Monitor threshold of errored frame period event	1 errored frame
Monitor window of link errored frame second statistics event	60s
Monitor threshold of link errored frame second statistics event	1s
Monitor window of link errored coding statistics event	1s
Monitor threshold of errored coding statistics event	1s
State of device fault indication	Enable
Local OAM event alarm function	Disable

9.1.4 Configuring basic functions of EFM

Configure basic functions of EFM for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`interface`** *`interface-type interface-number`*	Enter physical layer interface configuration mode.

Step	Command	Description
3	`Qtech(config-port)#`**`oam { active | passive }`**	Configure a working mode of EFM. ● Active: the QSW-8200 series switch actively initiates the OAM peer discovery process. In addition, the QSW-8200 series switch supports responding to remote loopback command and variable obtaining request. ● Passive: the QSW-8200 series switch does not initiate the OAM peer discovery process. In addition the QSW-8200 series switch does not support sending remote loopback command and variable obtaining request. By default, the QSW-8200 series switch is in passive mode. When configuring EFM OAM, you must ensure at least one end is in active mode. Otherwise, link detection will fail.

4	`Qtech(config-port)#`**`exit`**
	`Qtech(config)#`**`oam send-period`** `period-number`
		(Optional) OAM link connection is established by both ends sending INFO packet to each other. You can use this command to set the interval for sending INFO packets to control the communicate period of the link. The unit is set to 100ms. By default, the interval is set to 10 (10×100ms).

5	`Qtech(config)#`**`oam timeout`** *`period-number`*	(Optional) set the OAM link timeout. When the time for both ends on the OAM link failing to receive OAM packets exceeds the timeout, it believes that the OAM link is broken. The unit is set to second.
6	`Qtech(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
7	`Qtech(config-port)#`**`oam enable`**	Enable interface OAM. By default, OAM is disabled on the interface. Use the **oam disable** command to disable OAM on the interface.

9.1.5 Configuring EFM active function

Configure the EFM active function for the QSW-8200 series switch as below.

Note

The EFM active function can be configured only when the QSW-8200 series switch is in active mode.

(Optional) enabling EFM remote loop

Enable EFM remote loop for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical interface configuration mode.
3	Qtech(config-port)#**oam remote-loopback**	Configure the interface to start EFM remote loopback. Remote loopback can only be started after EFM connection is established and must be configured in active mode device.
4	Qtech(config-port)#**no oam remote-loopback**	(Optional) remote loopback is disabled. After loopback detection, disable remote loopback in time.

Note

Perform loopback detection periodically can discover network fault in time. Loopback detection in network sections can locate exact fault area and help users clear fault. In link loopback status, the QSW-8200 series switch sends back all packets except OAM packets received by the link to the peer device. Disable this function in time if no loopback detection is needed.

(Optional) configuring peer OAM event Trap

Configuring peer OAM event Trap for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**oam peer event trap enable**	Enable peer OAM event Trap so that link monitor events can be reported to the NMS in time. By default, the QSW-8200 series switch does not send Trap to the NMS through SNMP Trap when receiving peer link monitor event. Use the **oam peer event trap disable** command to disable this function.

(Optional) showing current variable information about peer device

Show current variable information about the peer device for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**show oam peer** [**link-statistic** | **oam-info**] [**port-list** *port-list*]	Obtain OAM information or interface statistics variable about the peer device.

Note

By obtaining the current variable of the peer, you can learn status of current link. IEEE802.3 Clause 30 defines and explains supported variable and its denotation obtained by OAM in details. The variable takes object as the maximum unit. Each object contains Package and Attribute. A package contains several attributes. Attribute is the minimum unit of a variable. When getting an OAM variable, it defines object, package, branch and leaf description of attributes by Clause 30 to describe requesting object, and the branch and leaf are followed by variable to denote object responds variable request. The QSW-8200 series switch supports obtaining OAM information and interface statistics.

Peer variable cannot be obtained until EFM is connected.

9.1.6 Configuring EFM passive function

Configure the EFM passive function for the QSW-8200 series switch as below.

Note

The EFM passive function can be configured regardless the QSW-8200 series switch is in active or passive mode.

(Optional) configuring the device to respond with EFM remote loop

Configure the QSW-8200 series switch to respond with EFM remote loop as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**oam loopback** { **ignore** | **process** }	Configure ignore or process EFM remote loopback. By default, the QSW-8200 series switch responds to EFM remote loopback.

Note

Peer EFM remote loopback will not take effect until the remote loopback process function is configured locally.

(Optional) configuring OAM link monitoring

Configure OAM link monitoring for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**oam errored-frame window** *window* **threshold** *threshold*	Configure errored frame monitor window and threshold. By default, the monitor window is 1s, and the threshold is 1 errored frame.
4	Qtech(config-port)#**oam errored-frame-period window** *window* **threshold** *threshold*	Configure errored frame period event monitor window and threshold. By default, the monitor window is 1000ms, and the threshold is 1 errored frame.
5	Qtech(config-port)#**oam errored-frame-seconds window** *window* **threshold** *threshold*	Configure link errored frame second window and threshold. By default, the monitor window is 60s, and the threshold is 1s.
6	Qtech(config-port)#**oam errored-symbol-period window** *window* **threshold** *threshold*	Configure errored code window and threshold. By default, the monitor window is 1s, and the threshold is 1s.

Note

OAM link monitor is used to detect and report link error in different conditions. When the detection link has a fault, the QSW-8200 series switch notifies the peer of the error generated time, window and threshold, etc. by OAM event, the peer receives event notification and reports the NMS through SNMP Trap. Besides, the local device can directly report events to the NMS center through SNMP Trap.

By default, the system has default values for error generated time, window and threshold setting.

(Optional) configuring OAM fault indication

Configure OAM fault indication for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.

Step	Command	Description
3	Qtech(config-port)#**oam notify** { **critical-event** | **dying-gasp** | **errored-frame** | **errored-frame-period** | **errored-frame-seconds** | **errored-symbol-period** } **disable** | **enable** }	Configure the OAM fault indication mechanism, which is used to inform the peer when the local device fails. Faults that can be notified to the peer include link-fault, dying-gasp, and critical-event. By default, OAM fault indication is enabled. When a fault occurs, the local device informs the peer through OAM. The link-fault must be notified to the peer while dying-gasp and critical-event can be disabled by using this command.

(Optional) configuring local OAM event trap

Configure local OAM event trap for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**oam event trap enable**	Enable local OAM event Trap to report link monitoring events to the NMS immediately. By default, local OAM event Trap is disabled. When detecting the link monitoring event, the QSW-8200 series switch does not inform the NMS through SNMP Trap. Use the **oam event trap disable** command to disable local OAM event Trap.

9.1.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show oam** [**port-list** *port-list*]	Show basic configurations of EFM.
2	Qtech#**show oam loopback** [**port-list** *port-list*]	Show configurations of EFM remote loopback configuration.
3	Qtech#**show oam notify** [**port-list** *port-list*]	Show configurations of OAM link monitor and fault indication.
4	Qtech#**show oam statistics** [**port-list** *port-list*]	Show OAM statistics.

No.	Command	Description
5	Qtech#**show oam trap** [**port-list** *port-list*]	Show configurations of OAM event Trap.
6	Qtech#**show oam event** [**port-list** *port-list*] [**critical**]	Show information about local critical fault detected by the interface.
7	Qtech#**show oam peer event** [**port-list** *port-list*] [**critical**]	Show information about local critical fault sent from the peer to the local interface.

9.1.8 Maintenance

Maintain the QSW-8200 series switch as below.

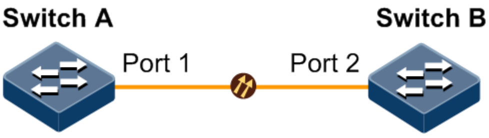
Command	Description
Qtech(config-port)#**clear oam statistics**	Clear statistics of OAM links on the interface.

9.1.9 Example for configuring EFM

Networking requirements

As shown in Figure 9-2, to improve Ethernet link management and maintenance capability between Switch A and Switch B, deploy EFM on the two Switch devices. Switch A is the active end while Switch B is the passive end. Deploy OAM event Trap on Switch A.

Figure 9-2 EFM networking



Configuration steps

Step 1 Configure the active end Switch A.

```
Qtech#hostname SwitchA
SwitchA#config
SwitchA(config)#interface port 1
SwitchA(config-port)#oam active
SwitchA(config-port)#oam enable
SwitchA(config-port)#oam event trap enable
SwitchA(config-port)#oam peer event trap enable
```

Step 2 Configure the passive end Switch B.

```
Qtech#hostname SwitchB
SwitchB#config
SwitchB(config)#interface port 1
SwitchB(config-port)#oam enable
```

Checking results

Use the **show oam** command to show EFM configurations on Switch A.

```
SwitchA#show oam port-list 1
Port: port 1
Mode:Active
Administrate state:  Enable
Operation state:     Disable
Max OAMPDU size:     1518
Send period:        1000 ms
Link timeout :       5 s
Config revision:     1
Supported functions:  Loopback, Event, Variable
```

Use the **show oam trap** command to show configurations of OAM event Trap on Switch A.

```
SwitchA#show oam trap port-list 1
Port:              port 1
Event trap:                         Enable
Peer event trap:                     Enable
Discovery trap total:                 0
Discovery trap timestamp:              0 days, 0 hours, 0 minutes
Lost trap total:                     0
Lost trap timestamp:                  0 days, 0 hours, 0 minutes
```

9.2 CFM (IEEE 802.1ag/ITU-Y.1731)

9.2.1 Introduction

Connectivity Fault Management (CFM) is a network-level Ethernet OAM technology, providing end-to-end connectivity fault detection, fault notification, fault judgement, and fault location. It is used to diagnose fault actively for Ethernet Virtual Connection (EVC), provide cost-effective network maintenance solution, and improve network maintenance through the fault management function.

The QSW-8200 series switch provides CFM that is compatible with both ITU-Y.1731 and IEEE 802.1ag standards.

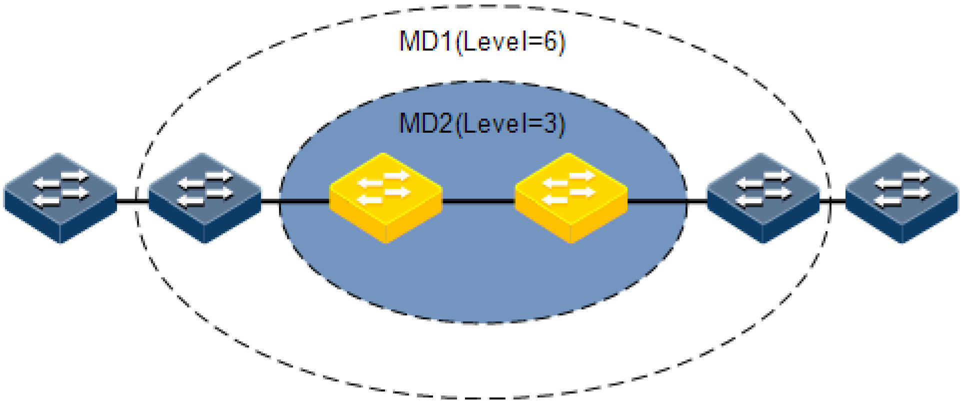
CFM consists of following components:

- MD

Maintenance Domain (MD), also called Maintenance Entity Group (MEG), is a network that runs CFM. It defines network range of OAM management. MD has a level property, with 8 levels (level 0 to level 7). The bigger the number is, the higher the level is and the larger the MD range is. Protocol packets in a lower-level MD will be discarded after entering a higher-level MD. If no Maintenance association End Point (MEP) but a Maintenance association Intermediate Point (MIP) is in a high-level MD, the protocol can traverse the higher-level MD. However, packets in a higher-level MD can traverse lower-level MDs. In the same VLAN range, different MDs can be adjacent, embedded, but not crossed.

As shown in Figure 9-3, MD 2 is in MD 1. Packets in MD 1 need to traverse MD 2. Configure MD 1 to be at level 6, and MD 2 to be at level 3. Then packets in MD 1 can traverse MD 2 and implement connectivity fault management of the whole MD 1. However, packets in MD 2 cannot diffuse into MD 1. MD 2 is a server layer while MD 1 is a client layer.

Figure 9-3 MDs at different levels



- Service instance

The service instance is also called Maintenance Association (MA). It is a part of a MD. One MD can be divided into one or multiple service instances. One service instance corresponds to one service and is mapped to a group of VLANs. VLANs of different service instances cannot cross. Though a service instance can be mapped to multiple VLANs, one service instance can only use a VLAN for sending or receiving OAM packets. This VLAN is the master VLAN of the service instance.

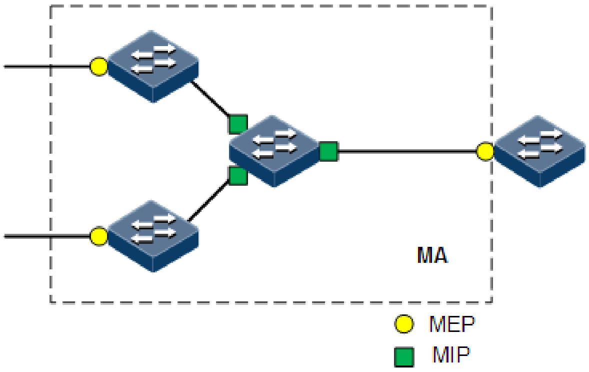
- MEP

As shown in Figure 9-4, the MEP is an edge node of a service instance. MEPs can be used to send and process CFM packets. The service instance and the MD where the MEP locates decide VLANs and levels of packets received and sent by the MEP.

For any device that runs CFM on the network, the MEP is called local MEP. For MEPs on other devices of the same service instance, they are called Remote Maintenance association End Points (RMEP).

Multiple MEPs can be configured in a service instance. Packets sent by MEPs in one instance take identical S-VLAN TAG, priority, and C-VLAN TAG. A MEP can receive OAM packets sent by other MEPs in the instance, intercept packets which at the same or lower level, and forward packets of higher level.

Figure 9-4 MEP and MIP



- MIP

As shown in Figure 9-4, the MIP is the internal node of a service instance, which is automatically created by the device. MIP cannot actively send CFM packets but can process and response to LinkTrace Message (LTM) and LoopBack Message (LBM) packets.

- MP

MEP and MIP are called Maintenance Point (MP).

9.2.2 Preparing for configurations

Scenario

To expand application of Ethernet technologies at a carrier-grade network, the Ethernet must ensure the same QoS as the carrier-grade transport network. CFM solves this problem by providing overall OAM tools for the carrier-level Ethernet.

CFM can provide following OAM functions:

- Fault detection (Continuity Check, CC)

The function is realized by periodically sending Continuity Check Messages (CCMs). One MEP sends CCM and other MEPs in the same service instance can verify the RMEP status when receiving this packet. If the QSW-8200 series switch fails or a link is incorrectly configured, MEPs cannot properly receive or process CCMs sent by RMEPs. If no CCM is received by a MEP during 3.5 CCM intervals, it is believed that the link fails. Then a fault Trap will be sent according to configured alarm priority.

- Fault acknowledgement (LoopBack, LB)

This function is used to verify the connectivity between two MPs through the source MEP sending LoopBack Message (LBM) and the destination MP sending LoopBack Reply (LBR). The source MEP sends a LBM to a MP who needs to acknowledge a fault. When receiving the LBM, the MP sends a LBR to the source MEP. If the source MEP receives this LBR, it is believed that the route is reachable. Otherwise, a connectivity fault occurs.

- Fault location (LinkTrace, LT)

The source MEP sends LinkTrace Message (LTM) to the destination MP and all MPs on the LTM transmission route will send a LinkTrace Reply (LTR) to the source MEP. By recording valid LTR and LTM, this function can be used to locate faults.

- Alarm Indication Signal (AIS)

This function is used to inhibit alarms when a fault is detected at the server layer (sub-layer, as shown in Figure 9-3). When detecting a fault, the MEP (including the server MEP) sends an AIS frame to the client MD. By transmitting ETH-AIS frames, the device can inhibit or stop an alarm on MEP (or server MEP).

When receiving an AIS frame, the MEP must inhibit alarms for all peer MEPs regardless of connectivity, because this frame does not include information about MEPs that are at the same level with the failed MEP. With AIS, the device can inhibit the alarm information at client level when the server layer (sub-layer) fails. Therefore, the network is easy for maintenance and management.

- Ethernet lock signal (Lock, LCK)

This function is used to notify managed lock and service interruption of server layer (sub-layer) MEPs. The data traffic is sent to a MEP that expects to receive it. This function helps the MEP that receives ETH-LCK frame to identify a fault. It is a managed lock action for server layer (sub-layer) MEP. Lock is an optional OAM management function. One typical scenario for applying this function is to perform detection when services are interrupted.

In general, CFM is an end-to-end OAM technology at the server layer. It helps reduce operation and maintenance cost. In addition, it improves the competitiveness of service providers.

Prerequisite

- Connect interfaces.
- Configure physical parameters to make interfaces Up at the physical layer.
- Create VLANs.
- Add interfaces to the VLAN.

9.2.3 Default configurations of CFM

Default configurations of CFM are as below.

Function	Default value
Global CFM status	Disable
Interface CFM status	Enable
MD status	Inexistent
MEP status based on service instance	Up direction
Storage time of errored CCM packets	100min
Status for MEP to send CCM packets	Not send
Internal for sending CCM packets	10s
Priority of CFM OAM packets	7

Function	Default value
Layer 2 ping status	The number of sending loopback packets is 3; the sending interval is 1s; the expiration time is 5s; the length of packet TLV is 64.
Switch status of the fault location database	Disable
Storage time of the fault location database	100min
AIS sending status	Disable
AIS sending period	1s
Alarm inhibition status	Enable
LCK packet sending status	Disable
Adding RDI flag to packets after the interface related to Up MEP becomes Down	Disable
DM&LM	Disable
MIP auto-creation	Enable

9.2.4 Enabling CFM

Enable CFM for the QSW-8200 series switch as below.

Note

CFM fault detection, location, etc. functions cannot take effect unless CFM is enabled.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**ethernet cfm enable**	Enable global CFM. By default, this function is disabled. Use the **ethernet cfm disable** command to disable this function.
3	Qtech(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode or aggregation group configuration mode.
4	Qtech(config-port)#**ethernet cfm enable**	Enable CFM on the interface. By default, this function is disabled. Use the **ethernet cfm disable** command to disable this function. After this function is disabled, the interface cannot receive or send CFM packets.
	Qtech(config-aggregator)#**ethernet cfm enable**	

9.2.5 Configuring basic CFM functions

Configure basic CFM functions for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**ethernet cfm domain** [**md-name** *domain-name*] **level** *level*	Create a MD. If a MD name is assigned by the **md-name** parameter, it indicates that the MD is in IEEE 802.1ag style. And all MAs and CCMs in the MD are in 802.1ag style. Otherwise, the MD is in Y.1731 style and all MAs and CCMs in the MD are in Y.1731 style. If a name is specified for a MD, the name must be unique in global. Otherwise the MD is configured unsuccessfully. Note Levels of different MDs must be different. Otherwise, the MD will fail to be configured.
3	Qtech(config)#**service** *cisid* **level** *level*	Create a service instance and enter service instance configuration mode. Character strings composed by MD name/service instance name are unique in global. If a service instance existed, you can use this command to enter service instance configuration mode directly. Note You cannot create two or more service instances with the same MDNAME+MANAME. When using the **no service ma-name level** *level* command, delete the MEP or manually created MIP if the MA contains a MEP or manually created MEP; otherwise, deletion will fail.

Step	Command	Description
4	Qtech(config-service)#**service vlan-list** *vlan-list* [**primary-vlan** *vlan-id*]	Configure VLAN mapping based on the service instance. The VLAN list contains up to 32 VLANs. If you do not use the **primary-vlan** parameter to specify the primary VLAN, the minimum VLAN is taken as the primary VLAN of the service instance. All MEPs in the service instance send and receive packets through this primary VLAN. **Note** The primary VLAN is used to send and receive packets. Therefore, all non-primary VLANs are mapped to the primary VLAN in logical. This logical VLAN mappingship is global, but VLANs cannot be crossed. For example, service instance 1 is mapped to VLANs 10–20 and service instance 2 is mapped to VLANs 15–30. Therefore, VLANs 15–20 are crossed. This configuration is illegal. The specified primary VLAN must be in the VLAN list.
5	Qtech(config-service)#**service mep** [**up** | **down**] **mpid** *mep-id* *interface-type* *interface-number* [**priority** *priority*]	Configure MEPs based on a service instance. When configuring a MEP based on a service instance, you must ensure that the service instance is mapped to a VLAN. By default, the MEP is Up. It indicates detecting the fault in uplink direction. **Note** In a MA, there is a remote end equal with the MEP ID. In a MA, the specified interface cannot contain manually configured MIP; otherwise, creation will fail. The UP MEP must be configured with a service distribution point; otherwise, it will not take effect. For details, see section 9.4 Service. The name of the service associated with CFM is MAID, namely MD Name+MA Name. The UP MEP must be configured with a static remote end before it takes effect. For a link aggregation interface, add an interface to it, associate CFM with it or configure it on the SDP interface, without supporting variable members of it. For the link aggregation interface based on the SDP interface, only one SDP interface can be configured.

Step	Command	Description
6	Qtech(config-service)#**service mip** *interface-type interface-number*	Configure MIP based on service instance.
7	Qtech(config-service)#**service mip auto-create enable**	Enable MIP automatic creation.
8	Qtech(config-service)#**service rdi mep** { **enable** | **disable** } **mep** { *mep-id* | **all** }	Enable/Disable adding RDI flag to packets after the interface related to Up MEP becomes Down. Note Only the UP MEP is supported. If CC sending is enabled on the UP MEP to be configured, the configuration will fail.
9	Qtech(config-service)#**service pm** { **enable** | **disable** } **mep** { *mep-id* | **all** }	Enable/Disable DM&LM. Note If CC sending is enabled on the UP MEP to be configured, the configuration will fail. If ACL resources are inadequate, the configuration will fail.

9.2.6 Configuring CFM fault detection

Configure CFM fault detection on the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**ethernet cfm errors archive-hold-time** *minute*	(Optional) configure the hold time of errored CCMs. Fault information reported by all MEPs is saved on the QSW-8200 series switch. By default, the hold time of errored CCMs is 100min. When a new hold time is configured, the system will detect the database immediately. The data will be removed if exceeds the time.
3	Qtech(config)#**service** *cisid* **level** *level*	Enter service instance configuration mode.
4	Qtech(config-service)#**service cc interval** { **1** | **10** | **60** | **600** | **3ms** | **10ms** | **100ms** }	(Optional) configure the interval for sending CCMs. By default, the interval for sending CCMs is 1s. The interval for sending CCM packets cannot be modified when CCM delivery is enabled.

Step	Command	Description
5	`Qtech(config-service)#`**`service cc enable mep`** `{` *`mep-list`* `|` **`all`** `}`	Enable MEPs sending CCMs. By default, MEPs do not sending CCMs. Use the **service cc disable mep** { *mepid-list* | **all** } command to disable sending CCMs.
6	`Qtech(config-service)#`**`service remote-mep`** *`mep-list`* **`port`** *`port-id`*	Configure the static RMEP.
7	`Qtech(config-service)#`**`service priority`** *`priority`*	(Optional) configure the priority of CFM OAM packet. After the priority is configured, CCMs, LBMs, LTMs, and DMMs sent by MEPs in a service instance will use the assigned priority. By default, the priority is set to 6. **Note** If the MEP is configured with packet priority, it uses the priority to send packets; otherwise, it uses the MA priority. The priority of LBR or LTR packets sent by the MEP is the same with that of received LBM or LTM packets. The configuration of interface CoS trust will modify the priority of CFM packets.
8	`Qtech(config-service)#`**`snmp-server trap cfm`** `{` **`all`** `|` **`ccmerr`** `|` **`macremerr`** `|` **`none`** `|` **`remerr`** `|` **`xcon`** `}` **`mep`** `{` **`all`** `|` *`mep-list`* `}`	(Optional) configure CFM permits sending fault trap type. CC function of CFM can detect fault in 5 levels, the order from high to low: level 5–cross connection, level 4-CCM error, level 3-loss of RMEP, level 2-interface status fault, level 1-RDI. By default, it is **macremerr**, namely permit fault trap on level 2-5. **Note** • When CFM detects a fault, faults at the identical level or lower levels will not generate trap again before the fault is cleared. • Wait for 10s until the fault status is cleared after CFM fault is removed.

9.2.7 Configuring fault acknowledgement

Configure CFM fault acknowledgement for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**service** *cisid* **level** *level*	Enter service instance configuration mode.
3	Qtech(config-service)#**ping** { *mac-address* | **mep** *rmep-id* } [**count** *count*] [**size** *size*] [**source** *mep-id*] [**interval** *interval*] [**timeout** *timeout*]	Perform Layer 2 Ping for acknowledging faults. By default, 5 LBMs are sent. The TLV length of a packet is set to 64. The QSW-8200 series switch automatically looks for an available source MEP. If Layer 2 Ping is performed with the destination MEP ID specified, CFM cannot finish Ping operation unless it finds the MAC address of the destination MEP based on the MEP ID. The source MEP will save RMEP data in the source MEP database after discovering and stabilizing the RMEP. And then according to MEP ID, the source MEP can find the MAC address of the RMEP in the RMEP database.
4	Qtech(config-service)#**ping ethernet multicast**	Conduct Layer 2 multicast. Use the **ping ethernet multicast** command to conduct Layer 2 multicast Ping. After a multicast Request packet is sent, the remote MEP learnt by CC will reply LBR or not. If local hardware CC is enabled, the local device records the remote MEP ID but not remote MEP MAC address. Then, you can obtain the MEP ID by querying TLV. If the MEP not learnt by CC replies with LBR packets, the MAC address is displayed without MEP ID.

Note

- Before executing this command, ensure that global CFM is enabled. Otherwise, the Ping operation will fail.
- If there is no MEP in a service instance, Ping operation will fail due to failing to find the source MEP.
- Ping operation will fail if the specified source MEP is invalid. For example, the specified source MEP does not exist or CFM is disabled on the interface where the specified source MEP is.
- The Ping operation will fail if it is performed based on the specified destination MEP ID and the MAC address of destination is not found based on the MEP ID.
- The Ping operation will fail if other users are using the specified source MEP to perform the Ping operation.

9.2.8 Configuring CFM fault location

Configure CFM fault location for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.

Step	Command	Description
2	Qtech(config)#**ethernet cfm traceroute cache enable**	(Optional) enable the traceroute cache switch. When the traceroute cache switch is enabled, you can use the **show ethernet cfm traceroute cache** command to view the route information saved through the database storage protocol. When the traceroute cache switch is disabled, the result will be automatically erased by the **traceroute** command. By default, the traceroute cache switch is disabled. Use the **ethernet cfm traceroute cache disable** command to
3	Qtech(config)#**ethernet cfm traceroute cache hold-time** *minute*	(Optional) configure the hold time of data in the traceroute cache. You can configure the hold time when the traceroute cache is enabled. By default, the hold time is set to 100min.
4	Qtech(config)#**ethernet cfm traceroute cache size** *size*	(Optional) configure the traceroute cache size. You can configure the traceroute cache size when the traceroute cache is enabled. By default, the traceroute cache size is set to 100. The data are not saved when the traceroute cache is disabled.
5	Qtech(config)#**service** *cisid* **level** *level*	Enter service instance configuration mode.
6	Qtech(config-service)#**traceroute** { *mac-address* | **mep** *mep-id* } [**ttl** *ttl*] [**source** *mep-id*] [**size** *size*]	Perform Layer 2 Traceroute for locating faults. By default, the TLV length of a packet is set to 64. The QSW-8200 series switch automatically looks for an available source MEP. If Layer 2 Traceroute is performed by specifying the destination MEP ID, CFM cannot finish Traceroute operation unless it finds the MAC address of the destination MEP based on the MEP ID. The source MEP will save RMEP data in the source MEP database after discovering and stabilizing the RMEP. And then according to MEP ID, the source MEP can find the MAC address of the RMEP in the RMEP database.

Note

- Before executing this command, ensure that global CFM is enabled. Otherwise, the Traceroute operation fails.
- If there is no MEP in a service instance, Traceroute operation will fail because of failing to find source MEP.
- Traceroute operation will fail if the specified source MEP is invalid. For example, the specified source MEP does not exist or CFM is disabled on the interface where the specified source MEP is.

- Traceroute operation will fail if the Ping operation is performed based on the specified destination MEP ID and the MAC address of destination is not found based on the MEP ID.
- Traceroute operation will fail if other users are using the specified source MEP to perform Traceroute operation.

9.2.9 Configuring alarm indication signal

- Configuring AIS on the server-layer device

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`service`** *`cisid`* **`level`** *`level`*	Enter service instance configuration mode.
3	`Qtech(config-service)#`**`service ais enable`**	Enable AIS delivery. By default, this function is disabled. Use the **service ais disable** command to disable this function.
4	`Qtech(config-service)#`**`service ais period`** `{` **`1`** `|` **`60`** `}`	Configure the AIS delivery period. By default, the period for sending AIS is set to 1s.
5	`Qtech(config-service)#`**`service ais level`** *`level`*	Configure the level of the customer layer MD to which AIS is sent.

- Configuring AIS on the customer-layer device

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`service`** *`cisid`* **`level`** *`level`*	Enter service instance configuration mode.
3	`Qtech(config-service)#`**`service suppress-alarms enable mep`** `{` **`all`** `|` *`mep-list`* `}`	Enable alarm inhibition. By default, this function is enabled. Use the **service suppress-alarms disable mep** *mepid* command to disable this function.

9.2.10 Configuring Ethernet lock signal

- Configuring Ethernet lock signal on the server-layer device

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`service`** *`cisid`* **`level`** *`level`*	Enter service instance configuration mode.

Step	Command	Description
3	`Qtech(config-service)#service lck start mep { all | mep-list }`	Enable sending function of LCK packet. By default, system disables LCK sending function. Use the **service lck stop mep** *mep-list* command to disable this function.
4	`Qtech(config-service)#service lck period { 1 | 60 }`	Configure the period for sending LCK packets. By default, the period for sending LCK packets is 1s.
5	`Qtech(config-service)#service lck level level`	Configure the level of LCK which is sent to client-level MD.

- Configuring Ethernet lock signal on the client-layer device

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#service cisid level level`	Enter service instance configuration mode.
3	`Qtech(config-service)#service suppress-alarms enable mep { all | mep-list }`	Enable alarm inhibition. By default, this function is enabled. Use the **service suppress-alarms disable mep** *mep-list* command to disable this function.

9.2.11 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Qtech#show ethernet cfm`	Show CFM global configurations.
2	`Qtech#show ethernet cfm domain [ level level ]`	Show configurations of MD and service instance.
3	`Qtech#show ethernet cfm errors [ level level ]`	Show errored CCM database information.
4	`Qtech#show ethernet cfm lck [ level level ]`	Show Ethernet locked signals.
5	`Qtech#show ethernet cfm local-mp [ interface port port-id | level level ]`	Show configurations of the local MEP.
6	`Qtech#show ethernet cfm remote-mep [ static [ level level ] ]`	Show static RMEP information.
7	`Qtech#show ethernet cfm remote-mep [ level level [ service name [ mpid local-mep-id ] ] ]`	Show RMEP discovery information.

No.	Command	Description
8	Qtech#**show ethernet cfm suppress-alarms** [**level** *level*]	Show configurations of CFM alarm inhibition.
9	Qtech#**show ethernet cfm traceroute-cache**	Show information about route discovery of the fault location database.
10	Qtech#**show ethernet cfm errors database** [**level** *level*]	Show AIS information.

9.2.12 Maintenance

Maintain the QSW-8200 series switch as below.

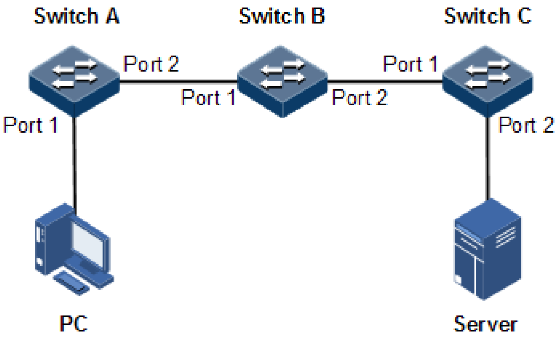
Command	Description
Qtech(config)#**clear ethernet cfm traceroute-cache**	Clear Traceroute Cache database.
Qtech(config)#**clear ethernet cfm errors datebase** [**level** *level*]	Clear errored database information.

9.2.13 Example for configuring CFM

Networking requirements

As shown in Figure 9-5, the PC communicates with the server through the network composed by Switch A, Switch B, and Switch C. You can deploy CFM feature on Switch devices to realize carrier-grade service level, namely, to realize active fault detection, acknowledgement and location. Switch A and Switch C are MEPs. Switch B is the MIP, detecting Ethernet fault from port 1 on Switch A to port 2 on Switch C. The MD level is 3.

Figure 9-5 CFM networking



Configuration steps

Step 1 Add interfaces into the VLAN.

Configure Switch A.

```
Qtech#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 100 active
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport access vlan 100
SwitchA(config-port)#exit
SwitchA(config)#interface port 2
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#exit
```

Configure Switch B.

```
Qtech#hostname SwitchB
SwitchB#config
SwitchB(config)#interface port 1
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#exit
SwitchB(config)#interface port 2
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#exit
```

Configure Switch C.

```
Qtech#hostname SwitchC
SwitchC#config
SwitchC(config)#create vlan 100 active
SwitchC(config)#interface port 2
SwitchC(config-port)#switch access vlan 100
SwitchC(config-port)#exit
SwitchC(config)#interface port 1
SwitchC(config-port)#switchport mode trunk
SwitchC(config-port)#exit
```

Step 2 Configure CFM fault detection.

Configure Switch A.

```
SwitchA(config)#ethernet cfm domain level 3
SwitchA(config)#service ma1 level 3
SwitchA(config-service)#service vlan-list 100
SwitchA(config-service)#service mep up mpid 301 port 1
SwitchA(config-service)#service remote-mep 302
SwitchA(config-service)#service cc enable mep all
SwitchA(config-service)#exit
SwitchA(config)#ethernet cfm enable
```

Configure Switch B.

```
SwitchB(config)#ethernet cfm domain level 3
SwitchB(config)#service ma1 level 3
SwitchB(config-service)#service vlan-list 100
SwitchB(config-service)#exit
SwitchB(config)#ethernet cfm enable
```

Configure Switch C.

```
SwitchC(config)#ethernet cfm domain level 3
SwitchC(config)#service ma1 level 3
SwitchC(config-service)#service vlan-list 100
SwitchC(config-service)#service mep up mpid 302 port 2
SwitchC(config-service)#service remote mep 301
SwitchC(config-service)#service cc enable mep all
SwitchC(config-service)#exit
SwitchC(config)#ethernet cfm enable
```

Step 3 Execute CFM fault acknowledgement.

Take Switch A for example.

```
Switch(config)#service ma1 level 3
Switch(config-service)#ping mep 302 source 301
Sending 5 ethernet cfm loopback messages to 001F.CE03.688d, timeout is
2.5 seconds:
!!!!!
Success rate is 100 percent (5/5).
Ping statistics from 001F.CE03.688d:
Received loopback replys:< 5/0/0 > (Total/Out of order/Error)
Ping successfully.
```

Step 4 Execute CFM fault location.

Take Switch A as an example.

```
SwitchA(config)#service ma1 level 3
SwitchA(config-service)#traceroute mep 302 source 301
TTL: <64>
Tracing the route to 001F.CE00.0002 on level 3, service ma1.
Traceroute send via port1.
-------------------------------------------------------------------------
---------
Hops  HostMac       Ingress/EgressPort  IsForwarded  RelayAction  NextHop
-------------------------------------------------------------------------
---------
 1    001F.CE00.0003      2/1        Yes        rlyFdb      001F.CE00.0003
 2    001F.CE00.0003      1/2        Yes        rlyFdb      001F.CE00.0001
3    001F.CE00.0001      1/-         No        rlyHit      001F.CE00.0002
```

Checking results

Use the **show ethernet cfm** command to show CFM configurations on the QSW-8200 series switch.

Take Switch A for example.

```
SwitchA#show ethernet cfm
Global CFM Admin Status: enable
Port CFM Enabled Portlist: P:1-28  PC:1-3
Archive hold time of error CCMs: 100(Min)
```

9.3 SLA

9.3.1 Introduction

SLA is a telecommunication service evaluation standard negotiated by the ISP and users. It is an agreement reached by both sides in service quality, priority, responsibility, etc.

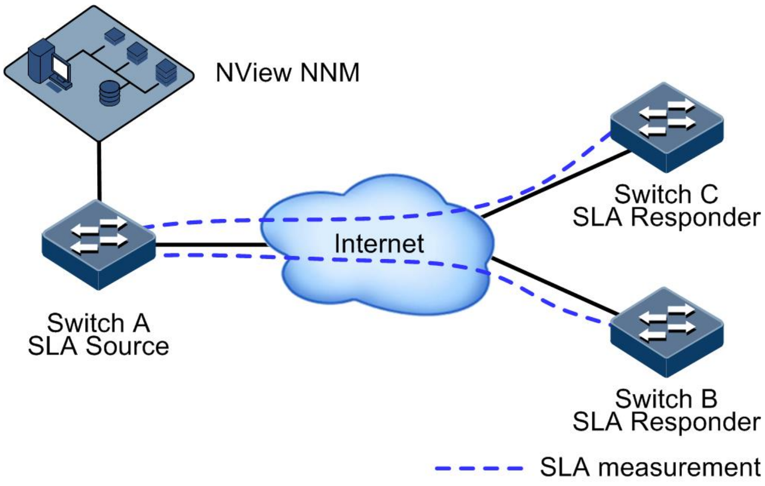
In technology, SLA is real-time network performance detection and statistics for responding time, network jitter, delay, packet loss rate, etc.

SLA principle

The SLA function implements end-to-end test, involving two ends:

- Source end: it sends the test packet, abstracts test data from the packet replied with by the destination end, and obtains test data through algorithms. It implements end-to-end performance test, including delay, jitter, and packet loss rate.
- Destination end: it replied the source end with the packet including test data.

Figure 9-6 SLA test networking



As shown in Figure 9-6, Switch A and Switch B are located in different spots but belong to the same user, and the user needs to test network performance between them. Configure SLA operation on Switch A with its destination address as Switch B, and then conduct scheduling to test network performance. In this way, the upper layer application (such as NMS) can obtain the roundtrip packet loss rate, roundtrip delay, and jitter through SLA statistics, and then analyze network performance and provide the user with required data.

Basic SLA concepts

- Operation

As a static concept, it is SLA network performance testing task from end to end, including jitter test/packet loss rate (Y1731-jitter/Y1731-pkt-loss) on the Layer 2 network and delay/jitter test (ICMP-echo/ICMP-jitter) on the Layer 3 network.

- Test

As a dynamic concept, it is used to describe an execution of one operation.

- Detection

As a dynamic concept, it is used to describe a procedure of transmitting-receiving packet in operation test. According to definition of operation, one operation test can contain multiple detections (a test contains only one detection for Echo operation).

- Schedule

As a dynamic concept, to describe a schedule of one operation, one schedule contains multiple periodical test execution.

- SLA operation type
  - Loss Measurement (LM) operation: used to test packet loss rate.
  - Delay Measurement (DM) operation: used to test delay and jitter.
- Network performance test indexes
  - Delay: the period between receiving the packet by the receiver and sending the packet by the sender
  - Jitter: the interval for receiving two adjacent packets minus the interval for sending these two adjacent packets
  - Packet loss rate: the ratio of the number of lost packets to the number of total sent packets, usually tested within throughput range

Supported SLA functions

Currently the QSW-8200 series switch supports the following SLA functions:

- Test Layer 2 network delay, jitter, and packet loss rate (Y1731-echo/Y1731-jitter/Y1731-pkt-loss). During Layer 2 network performance test, delay and jitter can be concurrently tested.
- Test Layer 3 network delay and jitter (icmp-echo/icmp-jitter).

The QSW-8200 series switch supports a maximum of 64 SLA operations and supports 64 concurrent scheduled operations.

9.3.2 Preparing for configurations

Scenario

The carrier and users sign SLA protocol to guarantee users can enjoy certain quality network service. To perform SLA protocol effectively, carrier needs to deploy SLA feature test performance on the device and the test result is evidence to ensure user's performance.

SLA feature chooses two testing node, configure SLA operation on one node and schedule executing it to implement network performance test between the two nodes.

Prerequisite

- Deploy CFM between the tested devices.
- Configure the IP address (scheduling of icmp-echo and icmp-jitter).

9.3.3 Limits on SLA configuration

There are limits on SLA configuration.

For topology:

- For 1:1 topology, the QSW-8200 series switch supports Up on both ends, Down on both ends, or Up on one end and Down on the other end.
- For 1:n topology, SLA configuration depends on different service instances.

For statistic values:

- In bandwidth statistics, the QSW-8200 series switch takes statistics of bandwidth based on Up MEP only.
- Services packets to be taken statistics of for packet loss rate must be known packets. The service packet VLAN and tested packet VLAN must be the same, and the service packet CoS must be the same with tested packet VLAN. For Up MEP, the statistics result is for service packets of the UNI interface. For Down MEP, the statistics result is for service packets of the NNI interface.
- Packet loss ratio is for service packets, so SLA protocol packets should not be discarded. If SLA protocol packets are discarded, packet loss rate cannot be tested.

9.3.4 Default configurations of SLA

Default configurations of SLA are as below.

Function	Default value
SLA operation scheduling status	Disable
SLA Layer 2 operation CoS	0
SLA Layer 3 operation service DSCP	0
Detection interval of SLA jitter operation	1s
Life period of SLA scheduling operation	forever
Test period of SLA scheduling operation	300s

Function	Default value
SLA alarm status	• Availability status change alarm: disabled • Threshold alarm status: disabled.

9.3.5 Creating SLA operation

Create an SLA operation for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**sla** *oper-num* **y1731-jitter remote-mep** *mep-id* **level** *level* **svlan** *vlan-id* [**cos** *cos-value*] [**interval** *period*] [**size** *size*]	(Optional) configure SLA Y1731-jitter operation according to the destination MEP.
3	Qtech(config)#**sla** *oper-num* **y1731-jitter remote-mac** *mac-address* **level** *level* **svlan** *vlan-id* [**cos** *cos-value*] [**interval** *period*] [**size** *size*]	(Optional) configure SLA Y1731-jitter operation according to the destination MAC address.
4	Qtech(config)#**sla** *oper-num* **y1731-pkt-loss slm remote-mac** *mac-address* **level** *level-id* **svlan** *vlan-id* [**cos** *cos-value*] [**interval** *interval-num*] [**size** *size*]	(Optional) configure SLA Y1731-pkt-loss operation according to the destination MAC address.
5	Qtech(config)#**sla** *oper-num* **y1731-pkt-loss slm remote-mep** *mep-num* **level** *level-id* **svlan** *vlan-id* [**cos** *cos-value*] [**interval** *interval-num*] [**size** *size*]	(Optional) configure SLA Y1731-pkt-loss operation according to the destination MEP.
6	Qtech(config)#**sla y1731-jitter quick-input** [**level** *level* [**svlan** *vlan-id*]	(Optional) quickly create a Y1731-jitter operation.
7	Qtech(config)#**sla** *oper-num* **icmp-echo dest-ipaddr** *ip-address* [**dscp** *dscp-value*]	(Optional) configure basic information about SLA ICMP-echo operation.
8	Qtech(config)#**sla** *oper-num* **icmp-jitter dest-ipaddr** *ip-address* [**dscp** *dscp-value*] [**interval** *period*]	(Optional) configure basic information about SLA icmp-jitter operation.

Note

After basic information about an operation is configured, the operation cannot be modified or reconfigured. If you need to modify the operation, delete the operation and then reconfigure it.

9.3.6 Configuring SLA scheduling

Configure SLA scheduling for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**sla schedule** *oper-num* [**life** { **forever** | *life-time* }] [**period** *period*]	Configure SLA operation scheduling information, and enable SLA operation scheduling.
3	Qtech(config)#**sla schedule** *oper-num* [**life** { **forever** | *life-time* }] [**period** *period*] **begin**	(Optional) configure automatical loading of SLA operation scheduling; namely, the QSW-8200 series switch automatically enables SLA operation scheduling upon startup.
4	Qtech(config)#**exit** Qtech#**write**	Configure and save auto-loading information.

Note

SLA supports up to 64 operations scheduled at a time, but waits a schedule period to finish an operation (reach schedule life time or stop schedule) before scheduling again or modifying schedule information.

9.3.7 Configuring SLA performance threshold profile

Configure the SLA performance threshold profile for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**sla-performance-tier** *template-id*	Create an SLA performance threshold profile, and enter SLA performance threshold profile configuration mode.
3	Qtech(config)#**description** *description*	Describe the SLA performance threshold profile.
4	Qtech(config)#**cos-lable** *cos-value* { **availability** *threshold* | **delay** *threshold* | **jitter** *threshold* | **loss-rate** *threshold* }	Configure thresholds for CoS-Lable packets.

9.3.8 Configuring SLA threshold

Configure SLA threshold for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**sla** *oper-num* **delay-threshold** *delay-threshod*	(Optional) configure delay threshold.
	Qtech(config)#**sla** *oper-num* **jitter-threshold** *jitter-threshod*	(Optional) configure jitter threshold.
3	Qtech(config)#**sla** *oper-num* **availability-threshold** *availability-threshod*	(Optional) configure availability threshold.
	Qtech(config)#**sla** *oper-num* **loss-rate-threshold** *loss-threshod*	(Optional) configure pass loss ratio threshold.

Note

A jitter operation allows configuring delay threshold and jitter threshold. A packet loss rate operation allows configuring packet loss rate threshold and availability threshold.

9.3.9 Configuring maintenance window

Configure the maintenance window for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**sla maintenance**{ **start** | **stop** }	Start/Stop the maintenance window of SLA operations.

9.3.10 Enabling alarms

Enable alarms for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**sla alarm availabilitychange enable**	(Optional) enable availability status change alarm.
3	Qtech(config)#**sla alarm threshold enable**	(Optional) enable threshold alarm.

9.3.11 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Qtech#show sla { all | oper-num } configuration`	Show SLA configuration.
2	`Qtech#show sla oper-num result`	Show test information about last SLA operation.
3	`Qtech#show sla oper-num { current | history } bins`	Show bins statistics of the delay operation.
4	`Qtech#show sla oper-num { current | history } statistics`	Show statistics of SLA operations.
5	`Qtech#show sla oper-num { avail-current | avail-history } statistics`	Show available statistics of the packet loss rate operation.
6	`Qtech#show sla oper-num threshold`	Show SLA operation threshold.
7	`Qtech#show sla alarm configuration`	Show configurations of SLA alarm.
8	`Qtech#show sla performance-tier [ profile-num ]`	Show properties of the maintenance window.

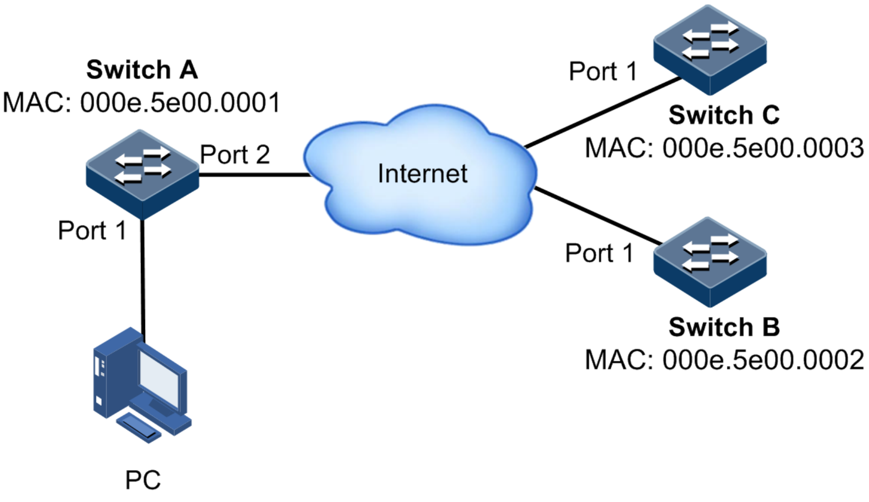
9.3.12 Example for configuring SLA

Networking requirements

As shown in Figure 9-7, SLA is deployed on the Switch, and is periodically scheduled to test the network performance between Switch A and Switch B, between Switch A and Switch C.

Conduct Layer 2 jitter test on Switch B towards Switch A. Conduct Layer 2 packet loss rate test on Switch C towards Switch A.

Figure 9-7 SLA test networking



Configuration steps

Step 1 Configure CFM on the Switch.

For details, see section 9.2.13 Example for configuring CFM.

Step 2 Configure y1731-jitter operation on Switch B, and enable operation scheduling.

```
SwitchB#config
SwitchB(config)#sla 1 y1731-jitter remote-mac 001f.ce00.0001 level 3
svlan 3
SwitchB(config)#sla schedule 2 life 20 period 10
```

Step 3 Configure y1731-pkt-loss operation on Switch C, and enable operation scheduling.

```
SwitchC#config
SwitchC(config)#sla 2 y1731-pkt-loss remote-mac 001f.ce00.0001 level 3
svlan 3
SwitchC(config)#sla schedule 2 life 20 period 10
```

Checking results

Use the **show sla configuration** command on Switch B to show SLA configurations.

```
Qtech#show sla 1 configuration
----------------------------------------------------------
Operation <1>:
   Type:               Y1731-JITTER
   Frame Type:          Delay Measurement
----------------------------------------------------------
   CoS:                0
   Service Vlan ID:      3
   MD Level:            3
   Remote DEST MAC:      001F.CE00.0001
   Timeout(sec):         1
   Jitter Interval(msec): 1000
   Measurement interval(sec):        10
   Schedule Life(sec):    20
   Schedule Status:      No Active
```

Use the **show sla configuration** command on Switch C to show SLA configurations.

```
QtechC#show sla 2 configuration
------------------------------------------------------------
Operation <2>:
   Type:               Y1731-PKT-LOSS
   Frame type:          LossMeasurement
------------------------------------------------------------
```

```
CoS:                0
Service Vlan ID:     3
MD Level:            3
Remote DEST MAC:      001F.CE00.0001
Timeout(sec):        1
Jitter Interval(msec): 1000
Measurement interval(sec):       10
Schedule Life(sec):   20
   Schedule Status:      Active
```

9.4 Service

9.4.1 Preparing for configurations

Scenario

The service is applied to four Ethernet services: E-Access, E-LAN, E-Line, and E-Tree. The service instance is configured for specified service types. The functions and features configured in the service instance can be viewed.

Prerequisite

N/A

9.4.2 Creating service instance of specified type

Create service instance of specified type for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#{ **eaccess** | **elan** | **eline** | **etree** } *service-name*	Create a service instance of a specified type, and enter service instance configuration mode.

9.4.3 Configuring service instance attributes

Configure service instance attributes for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**sdp** *interface-type interface-number* [**secondary**]	Configure the default primary Service Distribution Point (SDP) and secondary SDP.

Step	Command	Description
3	Qtech(config)#{ **eaccess** | **elan** | **eline** | **etree** } *service-name*	Create a service instance of a specified type, and enter service instance configuration mode. Note The name of CFM maintenance instance is MDNAME+MANAME.
4	Qtech(config-*service-name*)#**sap** *interface-type interface-number* [**leaf**]	Add a Service Access Point (SAP) to the service instance. The parameter **leaf** is configured in E-Tree service instance only.
5	Qtech(config-*service-name*)#**far-end remote-mep** *mep-id sap*	Configure the remote SAP of the service instance of the specified type.
6	Qtech(config-*service-name*)#**sdp vlan** *vlan-id*	Configure the service VLAN in the service instance of the specified type.
7	Qtech(config-*service-name*)#**sdp** *interface-type interface-number*	Add a SDP to the service instance of the specified type, and specify the interface. Note The interface should be a NNI interface and identical to the network side interface. For the link aggregation interface based on the SDP interface, only one SDP interface can be configured.
8	Qtech(config-*service-name*)#**customer** *description contact phone*	Add user information to the service instance.

9.4.4 Configuring CoS label

Configure the CoS label for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.

Step	Command	Description
2	`Qtech(config)#cos-label cos label`	Configure CoS label. CoS 1–8 correspond to CoS values 0–7. By default, CoS label is mapped with CoS value as below: • 1: Copper • 2: L2 • 3: Silver • 4: L1 • 5: H2 • 6: Gold • 7: H1 • 8: NC

9.4.5 Configuring service maintenance window

Configure the service maintenance window for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#{ eaccess | elan | eline | etree } service-name`	Enter service instance configuration mode.
3	`Qtech(config-service-name)#sla maintenance start-time HH:MM:SS stop HH:MM:SS`	Configure the service maintenance window.

9.4.6 Configuring SLA test

Configure the SLA test for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#{ eaccess | elan | eline | etree } service-name`	Enter service instance configuration mode.
3	`Qtech(config-service-name)#sla cos-label cos-label`	Configure CoS Label in the SLA test.
4	`Qtech(config-service-name)#sla remote-mep mep-list`	Configure the remote MEP in the service activation test.
5	`Qtech(config-service-name)#sla { start | stop }`	Start/Stop the SLA test.

9.4.7 Configuring loopback test in service instance

Configure the loopback test in service instance for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#{ eaccess | elan | eline | etree } service-name`	Enter service instance configuration mode.
3	`Qtech(config-service-name)#loopback { enable | diasble }`	Enable/Disable loopback.
4	`Qtech(config-service-name)#loopback ethertype HHHH`	Configure the type of the Ethernet protocol matching loopback.
5	`Qtech(config-service-name)#loopback remote-mep mep-list`	Configure the SAP interface corresponding to loopback.

9.4.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Qtech#show service service-name`	Show service instance status.
2	`Qtech#show service`	Show the service instance list.
3	`Qtech#show service service-name config`	Show configurations of service instance.
4	`Qtech#show service name performance remote-mep mep-list`	Show service performance of the remote MEP.

9.4.9 Example for configuring service instance

Networking requirements

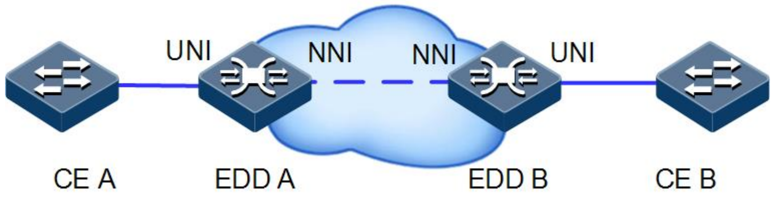
As shown in Figure 9-8, the user uses a MAN composed of EDD A and EDD B for communication between branches. To enable CE A and CE B of branches to communicate and make Ethernet link to carrier-grade CoS, deploy features such as VLAN, QinQ, CFM, and SLA on EDD A and EDD B. In this way, the network can implement user services and provide reliable OAM. Apply these features on Switch A and configure E-Line service on EDD A.

Configure Switch A as below:

- MD level: 3
- MA name: ma1

- Network side interface: port 25
- User side interface: port 1
- CFM VLAN: VLAN 100
- EDD A MEP IP: 301
- EDD B MEP IP: 302

Figure 9-8 Service networking



Configuration steps

Step 1 Add a user side interface to the VLAN, and configure QinQ.

```
EDDA#config
EDDA(config)#create vlan 100 active
EDDA(config)#interface port 1
EDDA(config-port)#switchport trunk native vlan 100
EDDA(config-port)#switchport vlan-mapping-miss discard
EDDA(config-port)#switchport qinq dot1q-tunnel
EDDA(config-port)#switchport vlan-mapping cvlan 1000-2000 add-outer 100
cos 5
EDDA(config-port)#exit
```

Step 2 Configure CFM.

```
EDDA(config)#ethernet cfm domain level 3
EDDA(config)#service ma1 level 3
EDDA(config-service)#service mip auto-create disable
EDDA(config-service)#service vlan-list 100 primary-vlan 100
EDDA(config-service)#service remote-mep 302 port 1
EDDA(config-service)#service mip port 25
EDDA(config-service)#service mep up mpid 301 port 1
EDDA(config-service)#service cc enable mep 301
EDDA(config-service)#exit
EDDA(config)#ethernet cfm enable
```

Step 3 Configure L2CP.

```
EDDA(config)#l2cp-profile 1
EDDA(config-l2cpprofile)#l2cp stp discard
EDDA(config-l2cpprofile)#l2cp slow-protocol peer
EDDA(config-l2cpprofile)#l2cp dot1x tunnel
EDDA(config-l2cpprofile)#exit
EDDA(config)#interface port 1
EDDA(config-port)#l2cp profile 1
EDDA(config-port)#exit
EDDA(config)#l2cp enable
```

Step 4 Configure hierarchical bandwidth guarantee.

```
EDDA(config)#bandwidth-profile 23 cir 30000 cbs 32 eir 70000 ebs 32
EDDA(config)#hierarchy-cos bandwidth-profile 1
EDDA(config-hcos)#bandwidth coslist 5 23
EDDA(config-hcos)#exit
EDDA(config)#bandwidth ingress port 1 vlan 100 23 hierarchy-cos 5
```

Step 5 Configure SLA.

```
EDDA(config)#sla 1 y1731-jitter remote-mep 302 level 3 svlan 100 cos 5
EDDA(config)#sla schedule 1 life forever period 300
```

Step 6 Configure service.

```
EDDA(config)#eline ma1
EDDA(config-service)#sap port 1
EDDA(config-service)#sdp vlan 100
EDDA(config-service)#sdp port 25
EDDA(config-service)#far-end remote-mep 302 2
EDDA(config-service)#exit
```

Checking results

Use the **show service** *service-name* command to shows E-Line configurations on the PE.

```
Qtech(config)#show service ma1
Point-to-Point EVC ma3
  CE-VLAN ID&CoS Preservation:  Yes
  Service Frame Delivery:      Ucast=Cond. Mcast=Uncond. Bcast=Uncond.
  CoS Label:                 Copper  Based on PCP
  Performance CoS Label:       Gold
  Service Distribution Point:  Vlan is 100, INNI is port25
UNI Qtech-port1
  Speed&Duplex:               Speed=10/100/1000Mbps auto. Duplex=Auto
  MAC Layer:                 MTU Size=9216 Frame Format=802.1Q
  Service Bundling:         All-to-One=No Multiplexing=No Bundling=Yes
  Default CE-VLAN ID:       0
  L2CP - MUST be forward:  E-LMI Lldp PTP-Peer-Delay GARP/MRP CDP VTP PAGP
                          UDLD PVST
  L2CP - MUST be tunneled:       802.1X
  L2CP - MUST be discarded:      STP Pause
  L2CP - MUST be peered:       LACP LAMP Link-OAM ESMC
EVC per UNI ma3-Qtech-port1 Root
  CE-Vlan mapping:           1-4094
  Ingress BWP per EVC:        CIR=30000Kbps CBS=32KB EIR=0Kbps EBS=0KB
                          CM=Color-Blind  CF=0
  CFM:                     Local MEP=301 CoS=7 CC=Enable PM=Disable
FarEnd 2
  Remote MEP:               302
```

Use the **show service config** command to show service configurations.

```
Qtech(config)#show service ma1 config
Service basic configuration information:
 eline ma1
 sap port 1
 sdp vlan 100
 sdp port 25
 far-end remote-mep 302 2
Service vlan configuration information:
 create vlan 100 active
 interface  port 1
 switchport trunk native vlan 100
 switchport trunk allowed vlan 100
 switchport mode trunk
 switchport vlan-mapping-miss discard
Service binding configuration information:
 interface  port 1
 switchport qinq dot1q-tunnel
 switchport vlan-mapping cvlan 1000-2000 add-outer 100 cos 5
L2cp configuration information:
 l2cp enable

 l2cp-profile 1
 l2cp stp discard
 l2cp slow-protocol peer
 l2cp dot1x tunnel
 interface  port 1
 l2cp profile 1
Bandwidth configuration information:
bandwidth-profile 23 cir 30000 cbs 32 eir 70000 ebs 32
 hierarchy-cos bandwidth-profile 1
bandwidth coslist 5 23
 bandwidth ingress port 1 vlan 100 1 hierarchy-cos 1
interface  port 1
 mls qos trust cos inner
Cfm configuration information:
 service remote-mep 302 port 1
 service mep up mpid 301 port 1
 service cc enable mep 301
Sla configuration information:
 sla 1 y1731-jitter remote-mep 302 level 3 svlan 100 cos 5
 sla schedule 1 life forever period 300
```

10 System management

This chapter describes basic principles and configurations of system management, and provides related configuration examples, including the following sections:

- SNMP
- KeepAlive
- RMON
- LLDP
- Extended OAM
- Optical module DDM
- Cable diagnosis
- Alarm management
- Hardware environment monitoring
- Fan monitoring
- CPU monitoring
- Caching CPU packets
- Dual systems
- Auto-Provisioning
- Checking device information
- Memory management
- Loopback
- Ping
- Traceroute

10.1 SNMP

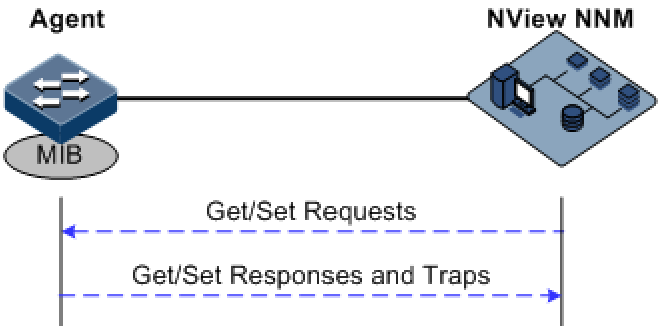
10.1.1 Introduction

Simple Network Management Protocol (SNMP) is designed by the Internet Engineering Task Force (IETF) to resolve problems in managing network devices connected to the Internet. Through SNMP, a network management system that can manage all network devices that support SNMP, including monitoring network status, modifying configurations of a network device, and receiving network alarms. SNMP is the most widely used network management protocol in TCP/IP networks.

Principle

A SNMP system consists of two parts: Agent and the NMS. The Agent and the NMS communicate through SNMP packets sent through UDP. Figure 10-1 shows the SNMP principle.

Figure 10-1 Principle of SNMP



The Qtech NMS can provide friendly Human Machine Interface (HMI) to facilitate network management. The following functions can be realized through it:

- Send request packets to the managed device.
- Receive reply packets and Trap packets from the managed device, and show result.

The Agent is a program installed on the managed device, realizing the following functions:

- Receive/reply request packets from the NMS
- To read/write packets and generate replay packets according to the packets type, then return the result to the NMS
- Define trigger condition according to protocol modules, enter/exit system or reboot the QSW-8200 series switch when conditions are satisfied; replying module sends Trap packets to the NMS through agent to report current status of the QSW-8200 series switch.

Note

An Agent can be configured with several versions, and different versions communicate with different NMSs. But SNMP version of the NMS must be consistent with that of the connected agent so that they can intercommunicate properly.

Version of protocol

Till now, SNMP has three versions: v1, v2c, and v3, described as below.

- SNMP v1 uses community name authentication mechanism. The community name, a string defined by an agent, acts like a secret. The network management system can visit the agent only by specifying its community name correctly. If the community name carried in a SNMP packet is not accepted by the QSW-8200 series switch, the packet will be dropped.
- Compatible with SNMP v1, SNMP v2c also uses community name authentication mechanism. SNMP V2c supports more operation types, data types, and errored codes, and thus better identifying errors.

- SNMP v3 uses User-based Security Model (USM) authentication mechanism. You can configure whether USM authentication is enabled and whether encryption is enabled to provide higher security. USM authentication mechanism allows authenticated senders and prevents unauthenticated senders. Encryption is to encrypt packets transmitted between the network management system and agents, thus preventing interception.

The QSW-8200 series switch supports v1, v2c, and v3 of SNMP.

MIB

Management Information Base (MIB) is the collection of all objects managed by NMS. It defines attributes for the managed objects:

- Name
- Access right
- Data type

The device-related statistic contents can be reached by accessing data items. Each proxy has its own MIB. MIB can be taken as an interface between NMS and Agent, through which NMS can read/write every managed object in Agent to manage and monitor the QSW-8200 series switch.

MIB stores information in a tree structure, and its root is on the top, without name. Nodes of the tree are the managed objects, which take a uniquely path starting from root (OID) for identification. SNMP protocol packets can access network devices by checking the nodes in MIB tree directory.

The QSW-8200 series switch supports standard MIB and Qtech-customized MIB.

10.1.2 Preparing for configurations

Scenario

To log in to the QSW-8200 series switch through the NMS, configure SNMP basic functions of the QSW-8200 series switch in advance.

Prerequisite

- Configure the IP address of the SNMP interface.
- Configure routing protocol, and make sure routing between QSW-8200 series switch and the NMS is available.

10.1.3 Default configurations of SNMP

Default configurations of SNMP are as below.

Function	Default value
SNMP view	By default: system, internet view
SNMP community	By default: public, private community IndexCommunityNameViewName Permission 1 public internet ro 2 private internet rw

Function	Default value
SNMP access group	By default: initialnone, initial group
SNMP user	By default: Qtechnone, Qtechmd5nopriv, Qtechshanopriv user
Mapping relation between SNMP user and access group	IndexGroupNameUserName SecModel 0 initialnone Qtechnone usm 1 initial Qtechmd5nopriv usm 2 initial Qtechshanopriv usm
Trap status	Enable
SNMP target host address	N/A

10.1.4 Configuring basic functions of SNMPv1/v2c

To protect itself and prevent its MIB from unauthorized access, the SNMP Agent proposes the concept of community. Management stations in the same community must use the community name in all Agent operations, or their requests will not be accepted.

The community name is used by different SNMP strings to identify different groups. Different communities can have read-only or read-write access permission. Groups with read-only permission can only query the device information, while groups with read-write access permission can configure the QSW-8200 series switch in addition to querying the device information.

SNMP v1/v2c uses the community name authentication scheme, and the SNMP packets of which the names are inconsistent to the community name will be discarded.

Configure SNMP v1, v2c for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`snmp-server view`** *`view-name oid-tree`* `[` *`mask`* `] {` **`included`** `|` **`excluded`** `}`	(Optional) create SNMP view and configure MIB variable range. By default, the view is internet, containing all MIB variables under the 1.3.6 node in the MIB tree.
3	`Qtech(config)#`**`snmp-server community`** *`com-name`* `[` **`view`** *`view-name`* `] {` **`ro`** `|` **`rw`** `}`	Create community name and configure the corresponding view and access permission. Use default view internet if **view** *view-name* option is empty.
4	`Qtech(config)#`**`snmp-server access`** *`group-name`* `[` **`read`** *`view-name`* `] [` **`write`** *`view-name`* `] [` **`notify`** *`view-name`* `] {` **`v1sm`** `|` **`v2csm`** `}`	(Optional) create and configure SNMP v1/v2c access group.

Step	Command	Description
5	`Qtech(config)#snmp-server group group-name user user-name { v1sm | v2csm | usm }`	(Optional) configure the mapping between user and access group. SNMP v1/v2c can assign the corresponding community group and configure secure model for groups. When the secure model is v1sm or v2csm, the secure level is noauthnopriv automatically.

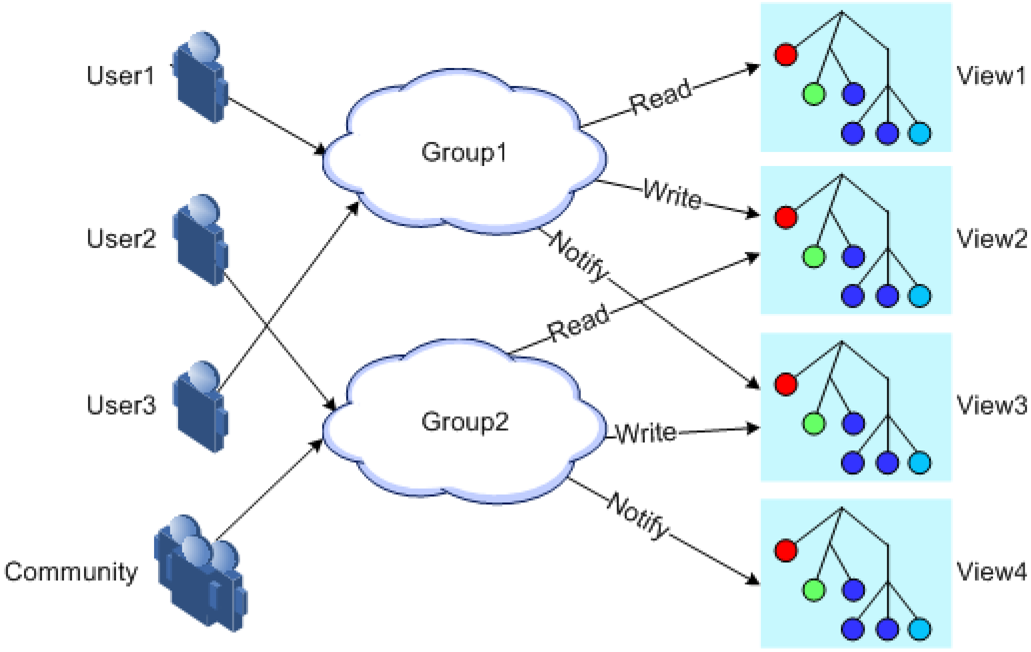
10.1.5 Configuring basic functions of SNMPv3

SNMPv3 uses USM over user authentication mechanism. USM comes up with the concept of access group: one or more users correspond to one access group, each access group sets the related read, write and announce view; users in access group have access permission in this view. The user access group to send Get and Set request must have permission corresponding to the request; otherwise the request will not be accepted.

As shown in Figure 10-2, the network management station uses the normal access from SNMP v3 to switch and the configuration is as below.

- Configure users.
- Check the access group to which the user belongs.
- Configure view permission for access groups.
- Create views.

Figure 10-2 SNMP v3 authentication mechanism



Configure SNMP v3 for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**snmp-server view** *view-name oid-tree* [*mask*] { **included** | **excluded** }	Create SNMP view and configure MIB variable range.
3	Qtech(config)#**snmp-server user** *user-name* [**remote** *engine-id*] **authentication** { **md5** | **sha** } *authpassword*	Create a user and configure authentication mode.
4	Qtech(config)#**snmp-server access** *group-name* [**read** *view-name*] [**write** *view-name*] [**notify** *view-name*] [**context** *context-name* { **exact** | **prefix** }] **usm** { **noauthnopriv** | **authnopriv** | **authpriv** }	Create a SNMP v3 access group and configure it.
5	Qtech(config)#**snmp-server group** *group-name* **user** *user-name* { **v1sm** | **v2csm** | **usm** }	Configure mapping between user and access group.

10.1.6 Configuring other information about SNMP

Configure other information about SNMP, including:

- Logo and contact method of administrators
- Physical location of the Switch

All SNMP v1, v2c and v3 are in support of the above configuration.

Configure other information about SNMP for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**snmp-server contact** *contact*	(Optional) configure logo and contact method of administrators. **Note** For example, use the Email as the log and contact for administrators.
3	Qtech(config)#**snmp-server location** *location*	(Optional) assign the physical location of the QSW-8200 series switch.

10.1.7 Configuring Trap

Note

Except for target host configuration, Trap configurations of SNMP v1, v2c, and v3 are identical.

A Trap is used by the QSW-8200 series switch to send unrequested information to the NMS automatically, which is used to report some critical events.

Finish the following tasks before configuring sending Trap:

- Configure SNMP basic function. SNMP v1 and v2c versions need to configure community name; SNMP v3 needs to configure username and SNMP view.
- Configure routing protocol, and make sure routing between QSW-8200 series switch and the NMS is available.

Configure sending Trap for SNMP for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface ip** *if-number*	Enter Layer 3 interface configuration mode.
3	Qtech(config-ip)#**ip address** *ip-address* [*ip-mask*] [**sub**] [*vlan-list*]	Configure Layer 3 interface IP address.
4	Qtech(config)#**exit**	Exit global configuration mode, and enter Privileged EXEC mode.
5	Qtech(config)#**snmp-server host** { *ip-address* | *ipv6-address* } **version 3** { **noauthnopriv** | **authnopriv** | **authpriv** } *user-name* [**udpport** *udpport*]	(Optional) configure the Trap target host over SNMPv3.
6	Qtech(config)#**snmp-server host** { *ip-address* | *ipv6-address* } **version** { **1** | **2c** } *com-name* [**udpport** *udpport*]	(Optional) configure the Trap target host over SNMP v1 and SNMP v2c.
7	Qtech(config)#**snmp-server enable traps**	Enable the QSW-8200 series switch to send Trap.

10.1.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech(config)#**show snmp access**	Show configurations of the SNMP access group.

No.	Command	Description
2	`Qtech(config)#show snmp community`	Show configurations of the SNMP community.
3	`Qtech(config)#show snmp config`	Show basic configurations of SNMP, including local SNMP engine ID, logo and contact method of administrators, Switch location and Trap switch status.
4	`Qtech(config)#show snmp group`	Show mapping between SNMP user and access group.
5	`Qtech(config)#show snmp host`	Show SNMP target host information.
6	`Qtech(config)#show snmp statistics`	Show SNMP statistics.
7	`Qtech(config)#show snmp user`	Show SNMP user information.
8	`Qtech(config)#show snmp view`	Show SNMP view information.

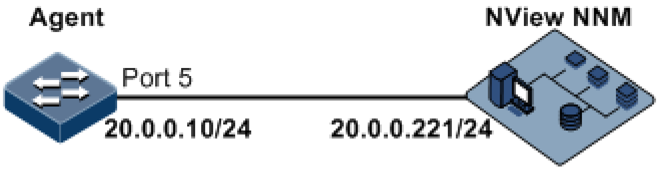
10.1.9 Example for configuring SNMP v1/v2c and Trap

Networking requirements

As shown in Figure 10-3, route between the NMS and the QSW-8200 series switch is available. The NMS can check the MIB under view corresponding to the remote Switch by SNMP v1/v2c, and the Switch can send Trap automatically to the NMS in emergency.

By default, there is VLAN 1 on the QSW-8200 series switch and all physical interfaces belong to VLAN 1.

Figure 10-3 SNMP v1/v2c networking



Configuration steps

Step 1 Configure the IP address of the QSW-8200 series switch.

```
Qtech#config
Qtech(config)#interface ip 0
Qtech(config-ip)#ipaddress 20.0.0.10 255.255.255.0 1
Qtech(config-ip)#exit
```

Step 2 Configure SNMP v1/v2c views.

```
Qtech(config)#snmp-server view mib2 1.3.6.1.2.1 included
```

Step 3 Configure SNMP v1/v2c community.

```
Qtech(config)#snmp-server community Qtech view mib2 ro
```

Step 4 Configure sending Trap.

```
Qtech(config)#snmp-server enable traps
Qtech(config)#snmp-server host 20.0.0.221 version 2c Qtech
```

Checking results

Use the **show interface ip** command to show configurations of the IP address.

```
Qtech#show interface ip
IF   Address       NetMask       Source     Catagory
----------------------------------------------------------
0    20.0.0.10  255.255.255.0  assigned   primary
```

Use the **show snmp view** command to show view configurations.

```
Qtech(config)#show snmp view
Index:    0
View Name: mib2
OID Tree:  1.3.6.1.2.1
Mask:     --
Type:     include
…
```

Use the **show snmp-server community** command to show community configurations.

```
Qtech#show snmp community
Index   Community Name     View Name         Permission
------------------------------------------------------------
1      private           internet          rw
2      public            internet          ro
3      Qtech          mib2            ro
```

Use the **show snmp host** command to show configurations of the target host.

```
Qtech#show snmp host
Index:         0
IP family:      IPv4
IP address:     20.0.0.221
Port:          162
User Name:      Qtech
SNMP Version:   v2c
Security Level: noauthnopriv
TagList:       bridge config interface rmon snmp ospf
```

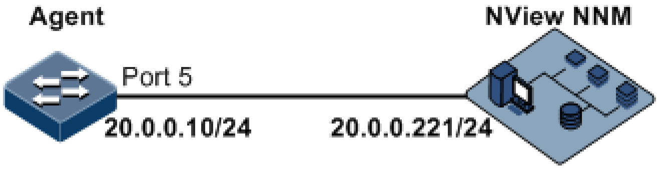
10.1.10 Example for configuring SNMP v3 and Trap

Networking requirements

As shown in Figure 10-4, route between the NMS and device is available, NMS monitors Agent by SNMP v3, and the switch can send Trap automatically to NMS when the Agent is in emergency.

By default, there is VLAN1 on the QSW-8200 series switch and all physical interfaces belong to VLAN 1.

Figure 10-4 SNMP v3 and Trap networking



Configuration steps

Step 1 Configure the IP address of the QSW-8200 series switch.

```
Qtech#config
Qtech(config)#interface ip 0
Qtech(config-ip)#ip address 20.0.0.10 255.255.255.0 1
Qtech(config-ip)#exit
```

Step 2 Configure SNMP v3 access.

Create access view mib2, including all MIB variables under 1.3.6.1.x.1.

```
Qtech(config)#snmp-server view mib2 1.3.6.1.2.1 1.1.1.1.0.1 included
```

Create user guestuser1, and use md5 authentication algorithm. The password is Qtech.

```
Qtech(config)#snmp-server user guestuser1 authentication md5 Qtech
```

Create a guest group access group. The security mode is usm, security level is authentication without encryption, and readable view name is mib2.

```
Qtech(config)#snmp-server access guestgroup read mib2 usm authnopriv
```

Configure guestuser1 user mapping to access group guestgroup.

```
Qtech(config)#snmp-server group guestgroup user guestuser1 usm
```

Step 3 Configure sending Trap.

```
Qtech(config)#snmp-server enable traps
Qtech(config)#snmp-server host 20.0.0.221 version 3 authnopriv guestuser1
```

Checking results

Use the **show snmp access** command to show configurations of the SNMP access group.

```
Qtech#show snmp access
…
  Index:        1
  Group:        guestgroup
  Security Model: usm
  Security Level: authnopriv
  Context Prefix: --
  Context Match:  exact
  Read View:     mib2
  Write View:    --
  Notify View:   internet
…
```

Use the **show snmp group** command to show mapping between users and access groups.

```
Qtech#show snmp group
Index   GroupName          UserName           SecModel
-----------------------------------------------------------
0       initialnone        none               usm
1       initial            md5nopriv          usm
2       initial            shanopriv          usm
3       guestgroup         guestuser1         usm
```

Use the **show snmp host** command to show configurations of the Trap target host.

```
Qtech#show snmp host
Index:        0
IP family:     IPv4
IP address:    20.0.0.221
Port:          162
User Name:     guestuser1
SNMP Version:   v3
Security Level: authnopriv
TagList:      bridge config interface rmon snmp ospf
```

10.2 KeepAlive

10.2.1 Introduction

The KeepAlive packet is a kind of KeepAlive mechanism running in High-level Data Link Control (HDLC) link layer protocol. The QSW-8200 series switch will send a KeepAlive packet to confirm whether the peer is online periodically to realize neighbor detection mechanism.

Trap is the unrequested information sent by the QSW-8200 series switch actively to the NMS, used to report some urgent and important events.

The Switch sends KeepAlive Trap actively which includes the basic information about RC551E (device name, device OID, MAC address and IP address) to the NMS. Network management synchronizes device information by IP to make the NMS discover fault in a short time, improve working efficiency and reduce working load of administrators.

10.2.2 Preparing for configurations

Scenario

The Switch sends KeepAlive packet to make network management discover network segment in a short time, improve working efficiency, and reduce the working load of administrators. You can configure the switch to enable or disable the KeepAlive transmission and its period. When enabled with KeepAlive Trap switch, set with snmp enable traps and Layer 3 IP address, the Switch will send a KeepAlive Trap alarm message to all target hosts with Bridge Trap every KeepAlive Trap Interval.

Prerequisite

- Configure the IP address of the SNMP interface.
- Configure basic functions of SNMP: SNMP v1 and v2c versions need to configure community name; SNMP v3 needs to configure username and SNMP view.
- Configure routing protocol, and make sure routing between the QSW-8200 series switch and the NMS is available.

10.2.3 Default configurations of KeepAlive

Default configurations of KeepAlive are as below.

Function	Default value
KeepAlive Trap status	Disable
KeepAlive Trap period	300s

10.2.4 Configuring KeepAlive

Configure KeepAlive for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`snmp-server keepalive-trap enable`**	Enable sending Trap for KeepAlive. By default, sending KeepAlive Trap packets is disabled. Use the **snmp-server keepalive-trap disable** command to disable this function.
3	`Qtech(config)#`**`snmp-server keepalive-trap interval`** *`period`*	(Optional) configure the period for sending Trap for KeepAlive.
4	`Qtech(config)#`**`snmp-server keepalive-trap pause`**	Configuring the pause function for KeepAlive.

Caution

To prevent multiple devices from sending Trap for KeepAlive in the same time according to the same period and causing heavy network management load, the real transmission period of KeepAlive Trap is timed as period+5s random transmission.

10.2.5 Checking configurations

Use the following commands to check configuration results.

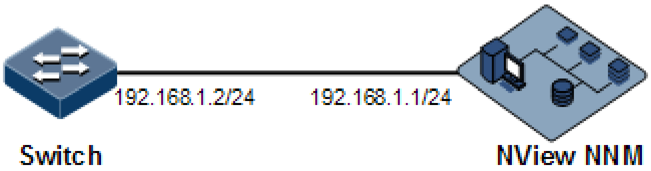
No.	Command	Description
1	`Qtech#`**`show keepalive`**	Show KeepAlive configurations.

10.2.6 Example for configuring KeepAlive

Networking requirements

As shown in Figure 10-5, the IP address of the Switch is 192.168.1.2, Trap target host address of SNMPv2c is 192.168.1.1, read and write community name is public, SNMP version is v2c. Configure time interval sending KeepAlive Trap from the Switch to SNMP network management station as 120s, and enable sending Trap for Keepalive.

Figure 10-5 KeepAlive networking



Configuration steps

Step 1 Configure the IP address of the Switch.

```
Qtech#config
Qtech(config)#interface ip 0
Qtech(config-ip)#ip address 192.168.1.2 255.255.255.0 1
Qtech(config-ip)#exit
```

Step 2 Configure the IP address of the Trap target host for SNMP.

```
Qtech(config)#snmp-server host 192.168.1.1 version 2c public
```

Step 3 Configure sending Trap for KeepAlive.

```
Qtech(config)#snmp-server keepalive-trap enable
Qtech(config)#snmp-server keepalive-trap interval 120
```

Checking results

Use the **show keepalive** command to show KeepAlive configurations.

```
Qtech#show keepalive
Keepalive Admin State:Enable
Keepalive trap interval:120s
Keepalive trap count:1
```

10.3 RMON

10.3.1 Introduction

Remote Network Monitoring (RMON) is a standard stipulated by Internet Engineering Task Force (IETF) for network data monitoring through different network Agents and NMS.

RMON is achieved based on SNMP architecture, including the NMS and the Agent running on network devices. On the foundation of SNMP, increase the subnet flow, statistics, and analysis to achieve the monitoring to one network segment and the whole network, while SNMP only can monitor the partial information about a single device and it is difficult for it to monitor one network segment.

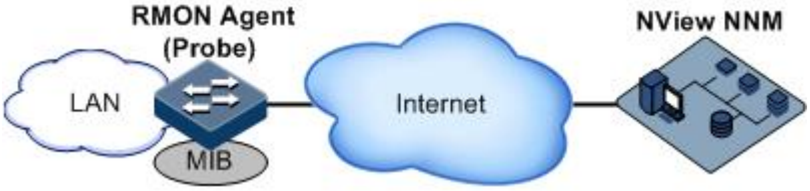
The RMON Agent is commonly referred to as the probe program. The RMON Probe can take the communication subnet statistics and performance analysis. Whenever it finds network failure, RMON Probe can report the NMS, and describes the capture information under unusual circumstances so that the NMS does not need to poll the device constantly. Compared with SNMP, RMON can monitor remote devices more actively and more effectively, network administrators can track the network, network segment or device malfunction more quickly. This method reduces the data flows between the NMS and Agent, makes it possible to manage large networks simply and powerfully, and makes up the limitations of SNMP in growing distributed Internet.

RMON Probe data collection methods:

- Distributed RMON. Network management center obtains network management information and controls network resources directly from RMON Probe through dedicated RMON Probe collection data.
- Embedded RMON. Embed RMON Agent directly to network devices (such as switches) to make them with RMON Probe function. Network management center will collect network management information through the basic operation of SNMP and the exchange data information about RMON Agent.

Qtech QSW-8200 series switch is embedded with RMON. As shown in Figure 10-6, the QSW-8200 series switch implements RMON Agent function. Through this function, the management station can obtain the overall flow, error statistics and performance statistics of this network segment connected to the managed network device interface so as to achieve the monitoring to one segment.

Figure 10-6 RMON networking



RMON MIB can be divided into nine groups according to function. Currently, there are four function groups achieved: statistics group, history group, alarm group, and event group.

- Statistic group: collect statistics on each interface, including receiving packets accounts and size distribution statistics.
- History group: similar with statistic group, it only collects statistics in an assigned detection period.
- Alarm group: monitor an assigned MIB object and set upper threshold and lower threshold in assigned time interval, trigger an event if the monitor object receives threshold value.
- Event group: cooperating with alarm group, when an alarm triggers an event, it records the event, such as sending Trap, write into log, etc.

10.3.2 Preparing for configurations

Scenario

RMON can help user monitor network and take statistics of traffic.

RMON is a more efficient monitoring method than SNMP. You need to assign alarm threshold, the QSW-8200 series switch over threshold will send trap information without variable information, which reduces communication amount between management device and managed device management and provides simple and efficient management to network.

Prerequisite

The link between the QSW-8200 series switch and the NMS is available.

10.3.3 Default configurations of RMON

Default configurations of RMON are as below.

Function	Default value
Statistics group	Enable all interfaces (including physical interfaces and Layer 3 interfaces) statistics.
History statistics group	Disable
Alarm group	N/A
Event group	N/A

10.3.4 Configuring RMON statistics

RMON statistics can take statistics on the interface, including sent and received packets, too small or too large packets, conflict, cyclic redundancy check and error count, packet loss, length of received packet, fragment, broadcast, multicast, and unicast messages.

Configure RMON statistics on the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`rmon statistics port-list`** *`port-list`* `[` **`owner`** *`owner-name`* `]`	Enable interface RMON statistics and configure related parameters. By default, RMON statistics on all interfaces is enabled. Use the **no rmon statistics** command to disable this function.

Note

After you use the **no rmon statistics** command to disable interface statistics, you cannot continue to obtain the interface statistics, but the interface still can take statistics.

10.3.5 Configuring RMON history statistics

Configure RMON history statistics for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**rmon history port-list** *port-list* [**shortinterval** *short-period*] [**longinterval** *long-period*] [**buckets** *buckets-number*] [**owner** *owner-name*]	Enable RMON history statistics on the interface and configure related parameters. Default, RMON history statistics on all interfaces is disabled. Use the **no rmon history** command to disable this function.

Note

After you use the **no rmon history** command to disable interface history statistics, the interface will not take data statistics and clear all history data collected previously.

10.3.6 Configuring RMON alarm group

Set one RMON alarm group instance (alarm-id) to monitor one MIB variable (mibvar). When the value of monitoring data exceeds the defined threshold, an alarm event will generate. Record the log to send Trap to network management station according to the definition of alarm event.

The monitored MIB variable must be real, and the data value type is correct. If the setting variable does not exist or value type variable is incorrect, return error. In the successfully setting alarm, if the variable cannot be collected later, close the alarm; reset if you wish to monitor the variable again.

By default, the triggered event number is 0; namely, no event will be triggered. If the number is not zero, and there is no corresponding configuration in event group, when the control variable is abnormal, it cannot trigger the event successfully until the event is established.

An alarm will be triggered as long as matching the condition when the upper or lower limit for one of the events is configured in the event table. If there is no configuration for the upper and lower limits related alarm event (rising-event-id, falling-event-id) in the event table, no alarm will not be generated even alarm conditions are met.

Configure the RMON alarm group on the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.

Step	Command	Description
2	Qtech(config)#**rmon alarm** *alarm-id mibvar* [**interval** *period*] { **absolute** | **delta** } **rising-threshold** *rising-value* [*rising-event-id*] **falling-threshold** *falling-value* [*falling-event-id*] [**owner** *owner-name*]	Add an alarm instance to the RMON alarm group, and configure related parameters.

10.3.7 Configuring RMON event group

Configure the RMON event group on the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**rmon event** *event-id* [**log**] [**trap**] [**description** *string*] [**owner** *owner-name*]	Add an event to the RMON event group, and configure related event processing mode.

10.3.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show rmon**	Show RMON configurations.
2	Qtech#**show rmon alarms**	Show information about the RMON alarm group.
3	Qtech#**show rmon events**	Show information about the RMON event group.
4	Qtech#**show rmon statistics** [**port** *port-id*]	Show information about the RMON statistics group.
5	Qtech#**show rmon history port** *port-id*	Show information about the RMON history statistics group.

10.3.9 Maintenance

Maintain the QSW-8200 series switch as below.

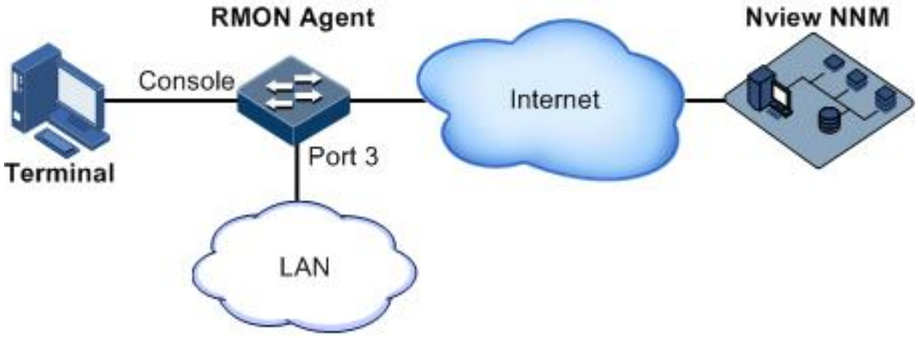
Command	Description
Qtech(config)#**clear rmon**	Clear all RMON configurations.

10.3.10 Example for configuring RMON alarm group

Networking requirements

As shown in Figure 10-7, the QSW-8200 series switch is the Agent, connected to terminal through Console interface, connected to remote NNM system through Internet. Enable RMON statistic function and statistic performance for port 3. When interface receiving packets exceeds the threshold in a period, record log and send Trap.

Figure 10-7 RMON networking



Configuration steps

Step 1 Create an event with index ID 10, used to record and send log information with description string High-ifOutErrors. The owner of log information is **system**.

```
Qtech#config
Qtech(config)#rmon event 1 log description High-ifOutErrors owner system
```

Step 2 Create an alarm item with index ID 10, used to monitor MIB variables 1.3.6.1.2.1.2.2.1.20.1. Check every 20s. If the variable increases by over 15, the Trap alarm will be triggered; the owner of alarm message is also **system**.

```
Qtech(config)#rmon alarm 10 1.3.6.1.2.1.2.2.1.20.1 interval 20 delta
rising-threshold 15 1 falling-threshold 0 owner system
```

Checking results

Use the **show rmon alarms** command to show whether there is event group event on the QSW-8200 series switch.

```
Qtech#show rmon alarms
Alarm 10 is active, owned by system
Monitors 1.3.6.1.2.1.2.2.1.20.1 every 20 seconds
Taking delta  samples, last value was 0
Rising threshold is 15, assigned to event 1
```

```
Falling threshold is 0, assigned to event 0
On startup enable rising and falling alarm
```

Use the **show rmon event**s command to show whether there is alarm group information on the QSW-8200 series switch.

```
Qtech#show rmon events
Event 1 is active, owned by system
Event generated at 0:0:0
Send TRAP when event is fired.
```

When an alarm event is triggered, you can also check related information in the alarm management part of the NMS.

10.4 LLDP

10.4.1 Introduction

With the enlargement of network scale and increase of network devices, the network topology becomes more and more complex and network management becomes very important. A lot of network management software adopts auto-detection function to trace changes of network topology, but most of the software can only analyze the Layer 3 network and cannot make sure the interfaces connect to other devices.

Link Layer Discovery Protocol (LLDP) is based on IEEE 802.1ab standard. Network management system can fast grip the Layer 2 network topology and changes.

LLDP organizes the local device information in different Type Length Value (TLV) and encapsulates in Link Layer Discovery Protocol Data Unit (LLDPDU) to transmit to straight-connected neighbour. It also saves the information from neighbour as standard Management Information Base (MIB) for network management system querying and judging link communication.

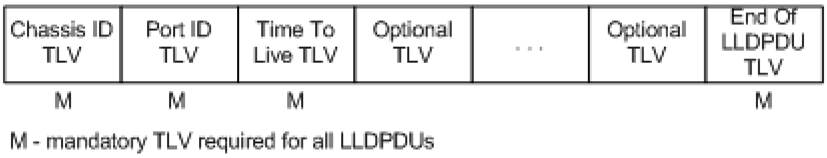
LLDP packet

The LLDP packet is to encapsulate LLDPDU Ethernet packet in data unit and transmitted by multicast.

LLDPDU is the data unit of LLDP. The device encapsulates local information in TLV before forming LLDPDU, then several TLV fit together in one LLDPDU and encapsulated in Ethernet data for transmission.

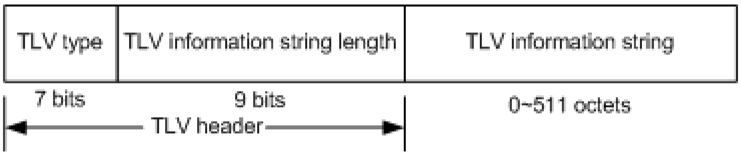
As shown in Figure 10-8, LLDPDU is made by several TLV, including 4 mandatory TLV and several optional TLV.

Figure 10-8 Structure of a LLDPDU



As shown in Figure 10-9, each TLV denotes a piece of information at local, such as device ID, interface number, etc. related Chassis ID TLV, Port ID TLV, and fixed TLV.

Figure 10-9 Structure of a TLV packet



TLV type value relationship is listed in Table 10-1, at present only types 0–8 are used.

Table 10-1 TLV types

TLV type	Description	Optional/Required
0	End Of LLDPDU	Required
1	Chassis ID	Required
2	Interface number	Required
3	Time To Live	Required
4	Interface description	Optional
5	System name	Optional
6	System description	Optional
7	System capabilities	Optional
8	Management address	Optional

Principle

LLDP is a kind of point-to-point one-way issuance protocol, which notifies local device link status to peer end by sending LLDPDU (or sending LLDPDU when link status changes) periodically from the local end to the peer end.

The procedure of packet exchange:

- When the local device transmits packet, it gets system information required by TLV from NMS (Network Management System) and gets configurations from LLDP MIB to generate TLV and form LLDPDU to transmit to peer.
- The peer receives LLDPDU and analyzes TLV information. If there is any change, the information will be updated in neighbor MIB table of LLDP and notifies the NMS.

When the device status is changed, the QSW-8200 series switch sends a LLDP packet to the peer. To avoid sending LLDP packet continuously because of device status changes frequently, you can set a delay timer for sending the LLDP packet.

The aging time of Time To Live (TTL) of local device information in the neighbour node can be adjusted by modifying the parameter values of aging coefficient, sends LLDP packets to neighbour node, after receiving LLDP packets, neighbour node will adjust the aging time of its neighbour nodes (sending side) information. Aging time formula, TTL = Min {65535, (interval × hold-multiplier)}:

- Interval indicates the time period to send LLDP packets from neighbor node.
- Hold-multiplier refers to the aging coefficient of device information in neighbor node.

10.4.2 Preparing for configurations

Scenario

When you obtain connection information between devices through the NMS for topology discovery, the QSW-8200 series switch needs to be enabled with LLDP, notifying their information to the neighbours mutually, and store neighbor information to facilitate the NMS queries.

Prerequisite

N/A

10.4.3 Default configurations of LLDP

Default configurations of LLDP are as below.

Function	Default value
Global LLDP status	Disable
Interface LLDP status	Enable
Delay sending timer	2s
Period sending timer	30s
Aging coefficient	4
Restart timer	2s
Alarm status	Enable
Alarm notification timer	5s

10.4.4 Enabling global LLDP

⚠Caution

Global LLDP cannot be enabled instantly after being disabled; it can be enabled again after the restart timer expires.

When you obtain connection information between devices through the NMS for topology discovery, the QSW-8200 series switch needs to be enabled with LLDP, notifying their information to the neighbours mutually, and store neighbor information to facilitate the NMS queries.

Enable global LLDP for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**lldp enable**	Enable global LLDP. By default, global LLDP is disabled. Use the **lldp disable** command to disable this function.

10.4.5 Enabling interface LLDP

Enable interface LLDP the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**lldp enable**	Enable interface LLDP. By default, interface LLDP is disabled. Use the **lldp disable** command to disable this function.

10.4.6 Configuring basic LLDP functions

Caution

When configuring the delay sending timer and period sending timer, the value of delay sending timer must be smaller than or equal to a quarter of the period for sending timer value.

Configure basic LLDP functions for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**lldp message-transmission interval** *period*	(Optional) configure period sending timer for LLDP packet. By default, it is 30s.

Step	Command	Description
3	Qtech(config)#**lldp message-transmission delay** *period*	(Optional) configure delay sending timer for LLDP packet. By default, it is 20s.
4	Qtech(config)#**lldp message-transmission hold-multiplier** *hold-multiplier*	(Optional) configure the aging coefficient of LLDP packets. By default, it is 4.
5	Qtech(config)#**lldp restart-delay** *period*	(Optional) configure restart timer. The device can be enabled with global LLDP again after the restart time when disabling global LLDP function. By default, it is 2s.

10.4.7 Configuring LLDP alarm

Enable LLDP alarm notification to send topology information update alarm to the NMS when the network changes.

Configure LLDP alarm for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**snmp-server lldp-trap enable**	Enable LLDP alarm function.
3	Qtech(config)#**lldp trap-interval** *period*	(Optional) configure the time for periodically sending LLDP Trap. By default, it is 5s.

Note

The period sending timer will send Trap if there is neighbour aging, new neighbour, neighbour information changing after LLDP alarm is enabled.

10.4.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show lldp local config**	Show LLDP local configurations.
2	Qtech#**show lldp local system-data** [**port** *port-id* | **port-channel** *port-channel-number*]	Show LLDP local system information.

No.	Command	Description
3	Qtech#**show lldp remote** [**port** *port-id* | **port-channel** *port-channel-number*][**detail**]	Show LLDP neighbor information.
4	Qtech#**show lldp statistic** [**port** *port-id* | **port-channel** *port-channel-number*]	Show statistics of LLDP packets.

10.4.9 Maintenance

Maintain the period sending timer as below.

Command	Description
Qtech(config)#**clear lldp statistic** *interface-type interface-number*	Clear LLDP statistics.
Qtech(config)#**clear lldp remote-table** *interface-type interface-number*	Clear LLDP neighbour information.

10.4.10 Example for configuring LLDP

Networking requirements

As shown in, the Switch is connected to NMS; enable LLDP between Switch A and Switch B, query Layer 2 link change through the NMS. The neighbor aging, new neighbor and neighbor information changes will be reported as LLDP alarms to the NMS.

Configuration steps

Step 1 Enable global LLDP and LLDP alarm.

Configure Switch A.

```
Qtech#hostname SwitchA
SwitchA#config
SwitchA(config)#lldp enable
SwitchA(config)#snmp-server lldp-trap enable
```

Configure Switch B.

```
Qtech#hostname SwitchB
SwitchB#config
SwitchB(config)#lldp enable
SwitchB(config)#snmp-server lldp-trap enable
```

Step 2 Configure the management IP address.

Configure Switch A.

```
SwitchA(config)#create vlan 1024 active
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport access vlan 1024
SwitchA(config-port)#exit
SwitchA(config)#interface ip 1
SwitchA(config-ip)#ip address 10.10.10.1 1024
```

Configure Switch B.

```
SwitchB(config)#create vlan 1024 active
SwitchB(config)#interface port 1
SwitchB(config-port)#switchport access vlan 1024
SwitchB(config)#interface ip 1
SwitchB(config-ip)#ip address 10.10.10.2 1024
```

Step 3 Configure LLDP attributes.

Configure Switch A.

```
SwitchA(config)#lldp message-transmission interval 60
SwitchA(config)#lldp message-transmission delay 9
SwitchA(config)#lldp trap-interval 10
```

Configure Switch B.

```
SwitchB(config)#lldp message-transmission interval 60
SwitchB(config)#lldp message-transmission delay 9
SwitchB(config)#lldp trap-interval 10
```

Checking results

Use the **show lldp local config** command to show local configurations.

```
SwitchA#show lldp local config
System configuration:
-------------------------------------------------------------------------
LLDP enable status: enable  (default is disabled)
LLDP enable ports: 1-28
LldpMsgTxInterval: 60     (default is 30s)
LldpMsgTxHoldMultiplier:4      (default is 4)
LldpReinitDelay: 2      (default is 2s)
LldpTxDelay: 2      (default is 2s)
```

```
LldpNotificationInterval:5     (default is 5s)
LldpNotificationEnable:enable  (default is enabled)
LldpNotificationEnable:           enable(default is enabled)
The destination mac address of LLDPDU: (default is 0180.c200.000e)
-------------------------------------------------------------
P1        :  destination-mac:0180.C200.000E
P2        :  destination-mac:0180.C200.000E
P3        :  destination-mac:0180.C200.000E
……

SwitchB#show lldp local config
System configuration:
-------------------------------------------------------------------------
LLDP enable status:enable  (default is disabled)
LLDP enable ports:1
LldpMsgTxInterval:60     (default is 30s)
LldpMsgTxHoldMultiplier:4     (default is 4)
LldpReinitDelay:2     (default is 2s)
LldpTxDelay:9     (default is 2s)
LldpNotificationInterval:10     (default is 5s)
LldpNotificationEnable:enable  (default is enabled)
```

Use the **show lldp remote** command to show neighbor information.

```
SwitchA#show lldp remote
Port  ChassisId         PortId       SysName  MgtAddress    ExpiredTime
-------------------------------------------------------------------------
P1  001F.CE02.B010    port 1       SwitchB 10.10.10.2    106
…
SwitchB#show lldp remote
Port  ChassisId         PortId       SysName  MgtAddress    ExpiredTime
-------------------------------------------------------------------------
P1  001F.CE12.F120    port 1       SwitchA 10.10.10.1    106
```

10.5 Extended OAM

10.5.1 Preparing for configurations

Scenario

Extended OAM is used to establish connection between Central Office (CO) device and remote device to achieve remote management.

Prerequisite

- Establish OAM link between devices to establish extended OAM link.
- The following configurations take the QSW-8200 series switch as the CO device. For different remote devices, the extended OAM networking situation and configuration

commands may be different; configure the QSW-8200 series switch according to the specific remote networking situation.

10.5.2 Default configurations of extended OAM

Default configurations of extended OAM are as below.

Function	Default value
OAM status	Disable
OAM working mode	Passive
Remote Trap status	Enable

10.5.3 Establishing OAM link

Note

You need to establish OAM link between devices to establish extended OAM link and both sides of devices are OAM active mode and passive mode respectively.

Establish OAM link on the CO device and remote device as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Qtech(config)#**oam** { **active** | **passive** }	Configure OAM working mode. Establish both sides of OAM link; configure the CO device to active mode and remote device to passive mode.
4	Qtech(config-port)#**oam enable**	Enable interface OAM.

10.5.4 Entering remote configuration mode

Note

The interface can enter remote configuration mode only when OAM link is established between CO device and remote device.

Enter remote configuration mode for the CO device as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.

Step	Command	Description
3	Qtech(config-port)#**remote-device**	Enter remote configuration mode.
4	Qtech(config-remote)#**interface client** *client-id* Qtech(config-remoteport)#	(Optional) enter remote interface configuration mode.

10.5.5 (Optional) showing remote extended OAM capacity

Caution

Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.

On the CO device, you can use the command of **show oam capability** to show remote device extended OAM capacity, and then take configuration according to the specific device.

Showe remote extended OAM capacity on the CO device as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**remote-device**	Enter remote configuration mode.
4	Qtech(config-remote)#**show oam capability**	Show remote device extended OAM management capacity.

10.5.6 Configuring remote host name

Note

Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.

Configure the remote host name on the CO device as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**remote-device**	Enter remote configuration mode.
4	Qtech(config-remote)#**hostname** *hostname*	Configure remote host name.

10.5.7 Configuring IP address of remote device

Note

Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.

Configure the IP address of the remote device as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**remote-device**	Enter remote configuration mode.
4	Qtech(config-remote)#**ip address** *ip-address* [*ip-mask*] *vlan-list*	Configure remote device IP address. Set the IP address of IP interface 0 on the remote device to take effect. IP address configuration needs to specify management VLAN, if this VLAN does not exist, create VLAN and take all interfaces as member interface by default; if associated VLAN exists, do not modify the member interface configuration.
5	Qtech(config-remote)#**ip default-gateway** *ip-address*	(Optional) configure remote device default gateway. The default gateway and configured IP address of IP interface 0 need to be in the same network segment.
6	Qtech(config-remote)#**management-port ip address** *ip-address* [*ip-mask*]	(Optional) configure the IP address of the out-of-band management interface for the remote device.

10.5.8 Configuring interface parameters on remote device

Note

Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.

Configure different remote interface parameters in different mode:

- In remote interface configuration mode, configure remote interface Up/Down, speed and working mode, etc.
- In remote configuration mode, configure remote interface auto-negotiation, interface bandwidth, and failover, etc.

Configuring interface parameters in remote interface configuration mode

In remote interface configuration mode, configure remote interface Up/Down, rate and working mode, etc.

Configure interface parameters in remote interface configuration mode as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**remote-device**	Enter remote configuration mode.
4	Qtech(config-remote)#**interface client** *client-id*	Enter remote interface configuration mode.
5	Qtech(config-remoteport)#**shutdown**	(Optional) shut down the remote interface.
6	Qtech(config-remoteport)#**speed** { **auto** | **10**| **100** }	(Optional) configure the interface rate on the remote device.
7	Qtech(config-remoteport)#**duplex** { **full** | **half** }	(Optional) configure remote device Client interface duplex mode. **Note** The OAM link maybe disconnect after configuring remote interface duplex mode.

Configuring interface parameters in remote configuration mode

In remote configuration mode, configure remote interface auto-negotiation, interface bandwidth, and failover, etc.

Configure interface parameters in remote configuration mode as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**remote-device**	Enter remote configuration mode.
4	Qtech(config-remote)#**line-speed auto**	(Optional) configure rate auto-negotiation on the Line interface of the remote device. You can configure the optical interface with auto-negotiation when the interface connecting remote device and CO device is the 1000 Mbit/s optical interface.

Step	Command	Description
5	Qtech(config-remote)#**rate-limit** *interface-type interface-number* **ingress** *rate*	(Optional) configure ingress bandwidth of the remote interface.
6	Qtech(config-remote)#**fault-pass enable**	(Optional) enable remote failover. The fault optical interface on the remote device changes to electrical port after being enabled with remote failover.

Note

For the above interface configuration in remote configuration mode:

- If the command line provides specified interface parameters, the corresponding configuration will take effect on specified interface;
- If the command line does not provide specified interface parameters, the corresponding configuration will take effect on all interfaces of the corresponding type on the remote device.

10.5.9 Configuring remote network management

Caution

Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.

Configuring remote network management

Configure remote network management for the CO device as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**remote-device**	Enter remote configuration mode.
4	Qtech(config-remote)#**snmp-server community** *community-name* { **ro** | **rw** }	Configure remote read/write community and read/write authority.

Configuring remote Trap

The remote device generates Trap information, which will be sent to CO device through OAM notification packet and then CO device will send the Trap to network management system.

To configure network management system to accept remote Trap, you need to enable remote Trap function on CO device and maybe enable to send extended OAM notification function on remote device.

Configure remote Trap for the CO device as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`snmp trap remote enable`**	Enable remote device to send Trap function.

Note

To configure remote Trap, some remote devices need to perform the command of **extended-oam notification enable** to enable to send extended OAM notification function in remote configuration mode.

10.5.10 Configuring remote VLAN

Caution

- Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.
- Different remote devices may have different configuration commands.

You can configure remote VLAN and process packets received by the remote device according to VLAN property configuration, such as set remote VLAN status, VLAN tag property and create remote VLAN group, etc.

Remote VLAN status:

- **dot1q**: remote VLAN mode is Dot1q; the packets entering device interface will be forwarded in accordance with dot1q mode.
- **forbid**: forbid remote VLAN function; the packets entering device interface will be forwarded in accordance with transparent transmission mode.
- **port**: remote VLAN is Port mode.

Enable remote VLAN CoS function, deal with the packets entering device interface according to VLAN priority, high priority first and low priority second.

Configure remote VLAN for the CO device as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`interface`** *`interface-type interface-number`*	Enter physical layer interface configuration mode.
3	`Qtech(config-port)#`**`remote-device`**	Enter remote configuration mode.

Step	Command	Description
4	Qtech(config-remote)#**vlan { dot1q | forbid | port }**	(Optional) configure remote VLAN status.
5	Qtech(config-remote)#**vlan cos enable**	(Optional) enable remote VLAN CoS.
6	Qtech(config-remote)#**vlan { cable-port | cpu-port | fiber-port } { tag | untag } priority** *priority* **pvid** *pvid*	(Optional) configure remote VLAN tag property.
7	Qtech(config-remote)#**vlan group** *group-id* **vid** *vid* **member-list** *member-list*	(Optional) create remote VLAN group.

10.5.11 Configuring remote QinQ

Note

Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.

Parameters for configure remote QinQ include switching mode, TPID, local VLAN, and access interface.

Configure remote QinQ for the CO device as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**remote-device**	Enter remote configuration mode.
4	Qtech(config-remote)#**switch-mode transparent**	(Optional) configure the remote device to work in full transparent transmission mode.
5	Qtech(config-remote)#s**witch-mode dot1q-vlan native-vlan** *vlan-id* [**line**]	(Optional) enable the remote device to work single Tag forwarding mode.
6	Qtech(config-remote)#**switch-mode double-tagged-vlan** [**tpid** *tpid*] **native-vlan** *vlan-id* [**line**]	(Optional) configure the remote device to work in double Tag forwarding mode.

Note

- To configure remote device to work in full transparent transmission mode, do not deal with data packets.

- To configure remote device to work in single Tag mode, after the QSW-8200 series switch is configured to single Tag mode, the data packets without Tag from user interface will be marked with Tag with local VLAN ID; do nothing if there is Tag.
- To configure remote device to work in double Tag mode, after the QSW-8200 series switch is configured to double Tag mode, the data packets without Tag from user interface will be marked with outer Tag with specified TPID and local VLAN ID.

10.5.12 Managing remote configuration files

Note

Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.

Manage remote configuration files on the CO device as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**remote-device**	Enter remote configuration mode.
4	Qtech(config-remote)#**write**	(Optional) save remote device configuration files in remote device flash.
5	Qtech(config-remote)#**write local**	(Optional) save remote device configuration files in CO device flash.
6	Qtech(config-remote)#**erase**	(Optional) delete remote device configuration files.

10.5.13 Rebooting remote device

Note

- During resetting or rebooting remote device, OAM link maybe disconnect and the CO device will not connect with remote device.
- Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.

Configuring rebooting the remote device on the CO device as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.

Step	Command	Description
3	Qtech(config-port)#**remote-device**	Enter remote configuration mode.
4	Qtech(config-remote)#**reboot**	Reboot remote device.

10.5.14 Checking configurations

Note

Whether the remote device supports the following items varies with the specific remote device. For details, see the corresponding manuals.

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech(config-remote)#**show remote-device information**	Show basic information about the remote device.
2	Qtech#**show extended-oam status** [**port-list** *port-list*]	Show extended OAM link status.
3	Qtech(config-remote)#**show interface port** [**detail** | **statistics**]	Show information about the remote device interfaces.
4	Qtech(config-remote)#**show vlan basic-information**	Show basic information about the remote device.
5	Qtech(config-remote)#**show vlan group-information** { **all** | *group-id* }	Show basic information about VLANs on the remote device.
6	Qtech#**show extended-oam statistics port-list** { **all** | *port-list* }	Show statistics of extended OAM frames.
7	Qtech#**show snmp trap remote**	Show remote Trap status.
8	Qtech#**show sfp**	Show information about the remote SFP module.

10.6 Optical module DDM

10.6.1 Introduction

Optical module Digital Diagnostics Monitoring (DDM) on the QSW-8200 series switch supports Small Form-factor Pluggable (SFP) and 10GE SFP+ diagnosis.

The fault diagnostics function of SFP provides the system a performance monitor method. The network administrator analysis the monitor data provided by SFP to predict the age of transceiver, isolate system fault and authenticate modules compatibility during installation.

The performance parameters of optical module which are monitored by optical module DDM are as below:

- Modular temperature
- Inner power voltage
- Tx offset current
- Tx optical power
- Rx optical power

When the performance parameters reach alarm threshold or status information changes, the corresponding Trap alarm will be generated.

10.6.2 Preparing for configurations

Scenario

Fault diagnostics f optical modules provide a detection method to SFP performance parameters; you can predict the service life of optical module, isolate system fault and check its compatibility during installation through analyzing monitoring data.

Prerequisite

N/A

10.6.3 Default configurations of optical module DDM

Default configurations of optical module DDM are as below.

Function	Default value
Global optical module DDM status	Disable
Interface optical module DDM status	Enable
Global optical module DDM sending Trap	Disable
Interface optical module DDM sending Trap	Enable

10.6.4 Enabling optical module DDM

Enable optical module DDM for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`transceiver ddm enable`**	Enable global optical module DDM. By default, optical module DDM is disabled. Use the **transceiver ddm disable** command to disable this function.

Step	Command	Description

3	`Qtech(config)#interface port port-id`
	`Qtech(config-port)#transceiver ddm enable`
		Enable interface optical module DDM. Only when global optical module DDM is enabled, the optical module enabling interface optical module DDM can take DDM.

10.6.5 Configuring sending Trap for optical module DDM

Configure sending Trap for optical module DDM for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#snmp-server trap transceiver enable`	Enable globally sending Trap for optical module DDM.

3	`Qtech(config)#interface port port-id`
	`Qtech(config-port)#transceiver ddm enable`
		Enable sending Trap for optical module DDM.
		Only when globally sending Trap for optical module DDM is enabled, the optical module, enabled with sending Trap for optical module DDM alarm, can send Trap when an alarm is generated.

10.6.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Qtech#show transceiver`	Show global switch status and interface switch status of optical module DDM.
2	`Qtech#show transceiver ddm port-list port-list [ detail ]`	Show optical module DDM performance parameters.
3	`Qtech#show transceiver port-list port-list history { 15m | 24h }`	Show history information about optical module DDM.
4	`Qtech#show transceiver information port-list port-list`	Show basic information about optical module.
5	`Qtech#show transceiver threshold-violations port-list port-list`	Show optical module over threshold information last time.

10.7 Cable diagnosis

10.7.1 Introduction

The QSW-8200 series switch support cable diagnosis for lines.

Cable diagnosis can yield the following results:

- Time of last cable diagnosis
- Detection result of the Tx cable
- Error location of the Tx cable
- Detection result of the Rx cable
- Error location of the Rx cable

10.7.2 Preparing for configurations

Scenario

By enabling cable diagnosis on the QSW-8200 series switch, you can learn the operation status of cables, and locate and clear faults, if any, in advance.

Prerequisite

N/A

10.7.3 Configuring fan monitoring

Configure fan monitoring for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`test cable-diagnostics port-list`** *`port-list`*	Enable cable diagnosis on the interface.

10.7.4 Checking configurations

Use the following commands to check configuration results.

Step	Command	Description
1	`Qtech#`**`show cable-diagnostics`** `[` **`port-list`** *`port-list`* `]`	Show information about cable diagnosis on the interface.

10.8 System log

10.8.1 Introduction

System Log function refers to that the QSW-8200 series switch records the system information and debugging information, etc. like logs and outputs them to assigned destination. When the QSW-8200 series switch has a fault, the system log facilitates you to view and locate fault.

The system message and some debug output information about the QSW-8200 series switch will be sent to system log. System log send the information to different destination according to user configuration, there are four kinds of destination to receive system log.

- Console interface: output log information to local Console through Console interface.
- Log host: output log information in log file format to log host.
- Monitor: output log information to monitor, such as telnet terminal.
- File: output log information to device Flash in log file format.
- Buffer: output log information to buffer.

The format of system log is as below.

```
timestamp  module-level- Packet content
```

The content of system log is as below.

```
FEB-22-2005 14:27:33  CONFIG-7-CONFIG:USER "Qtech"  Run "logging on"
FEB-22-2005 06:46:20  CONFIG-6-LINK_D: port 2 Link Down
FEB-22-2005 06:45:56  CONFIG-6-LINK_U: port 2 Link  UP
```

The system log information can be divided into eight levels according to the order of severity, as listed in Table 10-2.

Table 10-2 Log levels

Severity level	Level	Description
emergencies	0	The system is unavailable
alerts	1	Need to process immediately
critical	2	Critical status
errors	3	Error status
warnings	4	Alarm status
notifications	5	Normal but very important status
informational	6	Notification event
debugging	7	Debug information

Note

The severity level of output information can be set manually. According to the severity level, it only outputs low level or the same level configurations with severity level. For example, configure information output for specified level 3 (or assign the severity level errors directly); the level is 0 to 3, i.e. the information with severity level of emergencies–errors can be output.

10.8.2 Preparing for configurations

Scenario

The QSW-8200 series switch generates the key information, debugging information, error information, etc. to system log, outputs as log file or transmits to log host, Console interface or control console to facilitate you to check and locate the fault.

Prerequisite

N/A

10.8.3 Default configurations of system log

Default configurations of system log are as below.

Function	Default value
System log status	Enable
Output log information to console	Enable, the default level is information (6).
Output log information to host	N/A, the default level is information (6).
Output log information to file	Disable, the fixed level is warning (4).
Output log information to monitor	Disable, the default level is information (6).
Output log information to buffer	Disable, the default level is information (6).
Output log information to history list	Disable
Size of log history list	1
Transfer log to Trap	Disable, the default level is warning (4).
Log buffer size	4KB
Transmitting rate of system log	Unlimit
Timestamp of system log information	Debug: no timestamp to debug level (7) Syslog information.
	Log: the timestamp to 0-6 levels Syslog information is absolute time.

10.8.4 Configuring basic information about system log

Configure basic information about the system log for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#logging on`	(Optional) enable system log. By default, system log is enabled. Use the **no logging on** command to disable this function.
3	`Qtech(config)#logging time-stamp { debug | log } { datetime | none | uptime }`	(Optional) configure timestamp for system log. The optional parameter **debug** is used to assign debug level (7) system log timestamp; by default, this system log does not have timestamp The optional parameter **log** is used to assign debug level 0–6 system log timestamp; by default, this system log adopts date-time as timestamp.
4	`Qtech(config)#logging rate-limit` *`log-num`*	(Optional) configure transmitting rate of system log. By default, the rate is not limited.
5	`Qtech(config)#logging sequence-number`	(Optional) configure SN of system log. The SN only applies to control console, monitor station, log file and log buffer, but not log host and history list.
6	`Qtech(config)#logging discriminator` *`distriminator-number`* `{ facility | mnemonics | msg-body } { drops` *`key`* `| includes` *`key`* `| none }`	(Optional) create and configure system log filter. The filter can filter output log from control console, monitor station, log file and log buffer.

10.8.5 Configuring system log output

Configure system log output for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#config`	Enter global configuration mode.
2	`Qtech(config)#logging console [` *`log-level`* `| alerts | critical | debugging | emergencies | errors | informational | notifications | warnings | distriminator` *`discriminator-number`* `]`	(Optional) output system logs to the Console.

Step	Command	Description
3	Qtech(config)#**logging host** *ip-address* [*log-level* | **alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings** | **distriminator** *discriminator-number*]	(Optional) output system logs to the log host. Up to 10 log hosts are supported.
	Qtech(config)#**logging facility** { **alert** | **audit** | | **auth** | **clock** | **cron** | **daemon** | **ftp** | **kern** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **lpr** | **mail** | **news** | **ntp** | **sercurity** | **syslog** | **user** | **uucp** }	Configure the facility field of the log to be sent to the log host. Configuration may fail if you do not create the log host. This configuration is available for all log hosts configured on the QSW-8200 series switch.
4	Qtech(config)#**logging monitor** [*log-level* | **alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings** | **distriminator** *discriminator-number*]	(Optional) output system logs to the monitor.
5	Qtech(config)#**logging file** [**discriminator** *discriminateor-number*]	(Optional) output system logs to the Flash of the QSW-8200 series switch. Only warning-level logs are available.
6	Qtech(config)#**logging buffered** [*log-level* | **alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings** | **distriminator** *discriminator-number*]	(Optional) output system logs to the buffer.
	Qtech(config)#**logging buffered size** *size*	(Optional) configure the size of system log buffer.
7	Qtech(config)#**logging history**	(Optional) output system logs to the log history list. The level of the output logs is the one of the translated Trap.
	Qtech(config)#**logging history size** *size*	(Optional) configure the size of the log history list.
	Qtech(config)#**logging trap** [*log-level* | **alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings** | **distriminator** *discriminator-number*]	(Optional) enable translating specified logs in the history list to Traps. Configurations may fail if the system logs are not output to the log history list.

10.8.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Qtech#show logging`	Show configurations of system log.
2	`Qtech#show logging buffer`	Show information about system log buffer.
3	`Qtech#show logging discriminator`	Show filter information
4	`Qtech#show logging file`	Show contents of system log files.
5	`Qtech#show logging history`	Show the system log history list.

10.8.7 Maintenance

Maintain the QSW-8200 series switch as below.

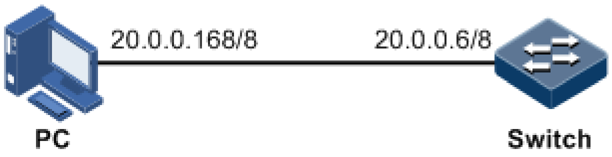
Command	Description
`Qtech#clear logging buffer`	Clear logs in the buffer.
`Qtech#clear logging file`	Clear log files.
`Qtech#clear logging statistics`	Clear log statistics.

10.8.8 Example for configuring outputting system logs to log host

Networking requirements

As shown in Figure 10-10, configure system log function, output device log information to log host for user to check.

Figure 10-10 Networking of outputting system log to log host



Configuration steps

Step 1 Configure the IP address of the QSW-8200 series switch.

```
Qtech#config
Qtech(config)#interface ip 0
Qtech(config-ip)#ip address 20.0.0.6 255.0.0.0 1
Qtech(config-ip)#exit
```

Step 2 Configure the system log to be output to the log host.

```
Qtech(config)#logging on
Qtech(config)#logging time-stamp log datetime
Qtech(config)#logging rate-limit 2
Qtech(config)#logging host 20.0.0.168 warnings
```

Checking results

Use the **show logging** command to show configurations of system log.

```
Qtech#show logging
Syslog logging:         enable
Dropped Log messages:    0
Dropped debug messages:  0
Rate-limited:           2 messages per second
Logging config:         disable
Logging config level:    informational(6)
Squence number display:  disable
Log time stamp:         datetime
Debug time stamp:       none
Log buffer size:        4kB
Debug level:            low
Syslog history logging:  disable
Syslog history table size:1
Dest     Status   Level          LoggedMsgs  DroppedMsgs  Discriminator
-------------------------------------------------------------------------
----
buffer   disable   informational(6)  0         0          0
console   enable   informational(6)  203        4          0
trap     disable  warnings(4)      0         0          0
file     disable  warnings(4)      0         0          0
monitor   disable   informational(6)  0         0          0
Log host information:
Max number of log server:    10
Current log server number:   1
Target Address    Port     Level          Facility      Sent     Drop
Discriminator
-------------------------------------------------------------------------
20.0.0.168       0       warnings(4)      local7       1       0       0
```

Show device log information output from emulation program interface on the PC.

10.9 Alarm management

10.9.1 Introduction

An alarm refers to information generated by the system based on module failures when a fault is generated on the QSW-8200 series switch or some working condition changes.

The alarm is used to report some urgent and important events and notify them to the network administrator promptly, which provides strong support for monitoring device operation and diagnosing faults.

The alarm is stored in the alarm buffer. Meanwhile, the alarm is generated to log information. If the NMS is configured, the alarm will be sent to it through SNMP. The information sent to the NMS is called Trap.

Classification of alarms

There are 3 kinds of alarms according to properties of an alarm:

- Fault alarm: alarms generated because of hardware failure or anomaly of important functions, such as port Down alarm
- Recovery alarm: alarms generated when device failure or abnormal function returns to normal, such as port Up alarm;
- Event alarm: prompted alarms or alarms that are generated because the fault alarm and recovery alarm cannot be related, such as alarms generated because of failing to Ping.

Alarms are divided into 5 types according to functions:

- Communication alarm: alarms related to the processing of information transmission, including alarms generated because of communication failure between Network Elements (NEs), NEs and NMS, or NMS and NMS
- Service quality alarm: alarms caused by service quality degradation, including congestion, performance decline, high resource utilization rate, and the bandwidth reducing
- Processing error alarm: alarms caused by software or processing errors, including software errors, memory overflow, version mismatching, and abnormal program aborts
- Environmental alarm: alarms caused by equipment location-related problems, including the temperature, humidity, ventilation. and other abnormal working conditions
- Device alarm: alarms caused by failure of physical resources, including the power supply, fan, processor, clock, input/output interface, and other hardware.

Alarm output

There are 3 alarm output modes:

- Alarm buffer: alarms are recorded in tabular form, including the current alarm table and history alarm table.
  - Current alarm table: records alarms which are not cleared, acknowledged or restored.
  - History alarm table: consists of acknowledged and restored alarms, recording the cleared, auto-restored, or manually acknowledged alarms.
- Log: alarms are generated to system log when recorded in the alarm buffer, and stored in the alarm log buffer.
- Trap: alarms sent to the NMS when the NMS is configured

Alarms will be broadcasted according to various terminals configured on the QSW-8200 series switch, including CLI terminal and the NMS.

Log output of alarms starts with the symbol "#", and the output format is:

```
#Index TimeStamp HostName ModuleName/Severity/name:Arise From Description
```

Table 10-3 lists alarm fields.

Table 10-3 Alarm fields

Field	Description
Index	Alarm index
TimeStamp	Time when an alarm is generated
HostName	Name of the host generating alarms
ModuleName	Name of a module that generates an alarm
Severity	Alarm level
Name	Alarm name
Arise From Description	Descriptions about an alarm

Alarm levels

The alarm level is used to identify the severity degree of an alarm. The level is defined in Table 10-4.

Table 10-4 Alarm levels

Level	Description	Syslog
Critical (3)	This alarm has affected system services and requires immediate troubleshooting. Restore the device or source immediately if they are completely unavailable, even it is not during working time.	1 (Alert)
Major (4)	This alarm has affected the service quality and requires immediate troubleshooting. Restore the device or source service quality if they decline; or take measures immediately during working hours to restore all performances.	2 (Critical)
Minor (5)	This alarm has not influenced the existing service yet, which needs further observation and take measures at appropriate time so as to avoid more serious fault.	3 (Error)

Level	Description	Syslog
Warning (6)	This alarm will not affect the current service, but maybe the potential error will affect the service, so it can be considered as needing to take measures.	4 (Warning)
Indeterminate (2)	Uncertain alarm level, usually the event alarm.	5 (Notice)
Cleared (1)	This alarm shows to clear one or more reported alarms.	5 (Notice)

Related concepts

Related concepts about alarm management are displayed as follows:

- Alarm inhibition

The QSW-8200 series switch only records root-cause alarms but incidental alarms when enabling alarm inhibition. For example, the generation of alarm A will inevitably produce alarm B, then alarm B is inhibited and does not appear in the alarm buffer or record the log information when enabling alarm inhibition. By enabling alarm inhibition, the QSW-8200 series switch can effectively reduce the number of alarms.

The root-cause alarm and all other incidental alarms will be recorded on the QSW-8200 series switch when alarm inhibition is disabled.

- Alarm auto-reporting

Auto-report refers that an alarm will be reported to the NMS automatically with its generation and the NMS does not need to query or synchronize alarms actively.

You can set auto-reporting to some alarm, some alarm source, or the specified alarm from specified alarm source.

Note

The alarm source refers to an entity that generates related alarms, such as interfaces, devices, or cards.

- Alarm monitoring

Alarm monitoring is used to process alarms generated by modules:

  - When alarm monitoring is enabled, the alarm module will receive alarms generated by modules, and process them according to configurations of the alarm module, such as recording alarm in the alarm buffer, or recording system logs, etc.;
  - When alarm monitoring is disabled, the alarm module will discard alarms generated by modules without follow-up treatment. In addition, alarms will not be recorded on the QSW-8200 series switch.

You can perform alarm monitoring on some alarm, alarm source, or specified alarm from specified alarm source.

- Alarm reverse mode

Alarm reverse refers to the device will report the information opposite to actual status when recording alarm information, or report the alarm when there is no alarm information. Not report if there is alarm information.

Currently, the device is only in support of reverse mode configuration of the interface. There are three reverse modes to be set; the specific definitions are as follows:

- Non-reverse mode

Device alarm is reported normally.

- Manual reverse mode

Set the alarm reverse mode of an interface as manual reverse mode, then no matter what the current alarm state is, the reported alarm state of the interface will be changed opposite to the actual alarm state immediately, that is to say, not report when there are alarms, report when there are not alarms actually. The interface will maintain the opposite alarm state regardless of the alarm state changes before the alarm reverse state being restored to non-reverse mode.

- Auto-reverse mode

Set the alarm reverse mode as auto-reverse mode. If the interface has not actual reverse alarm currently, the setting will return fail; if the interface has actual reverse alarm, the setting is success and enter reverse mode, i.e. the interface reported alarm status is changed opposite to the actual alarm status immediately. After the alarm is finished, the enabling state of interface alarm reverse will ends automatically and changes to non-reverse alarm mode so that the alarm state can be reported normally in next alarm.

- Alarm delay

Alarm delay refers that the QSW-8200 series switch will record alarms and report them to the NMS after a delay but not immediately when alarms generate. Delay for recording and reporting alarms are identical.

By default, an alarm is reported after 5 seconds it is generated and an alarm is cleared after 5 seconds it is finished.

- Alarm storage mode

Alarm storage mode refers to how to record new generated alarms when the alarm buffer is full. There are two ways:

- **stop**： stop mode, when the alarm buffer is full, new generated alarms will be discarded without recording.
- **loop**: loop mode, when the alarm buffer is full, the new generated alarms will replace old alarm information and take rolling records.

The current alarm list can record up to 1000 alarms and the historical alarm table can record up to 500 alarms. Use the configured storage mode to process newly-generated alarms when the alarm table is full.

- Clearing alarms

Clear the current alarm, which means deleting current alarms from the current alarm table. The cleared alarms will be saved to the historical alarm table.

- Viewing alarms

The administrator can view alarms and monitor alarms directly on the QSW-8200 series switch. If the QSW-8200 series switch is configured with the NMS, the administrator can monitor alarms on the NMS.

10.9.2 Preparing for configurations

Scenario

When the QSW-8200 series switch fails, alarm management module will collect fault information and output alarm occurrence time, alarm name and description information in log format to help you locate problem quickly.

If the QSW-8200 series switch is configured network management system, alarm information can be reported directly to the network management system, providing possible alarm causes and treatment recommendations to help you process fault.

Alarm management makes it easy for the user to take alarm inhibition, alarm auto-reporting, alarm monitoring, alarm reverse, alarm delay, alarm memory mode, alarm clear and alarm view directly on the QSW-8200 series switch.

Prerequisite

N/A

10.9.3 Default configurations of alarm management

Default configurations of alarm management are as below.

Function	Default value
Alarm inhibition	Enable
Alarm monitoring	All enable
Alarm auto-reporting	All auto-reporting
Alarm reverse mode	Non-reverse
Alarm delay time	0s
Alarm memory mode	Stop
Alarm output system log	Enable

10.9.4 Configuring basic alarm functions

Configure basic alarm function for the QSW-8200 series switch as below.

All following steps are optional and in any sequence.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`alarm inhibit enable`**	Enable alarm inhibition.
3	`Qtech(config)#`**`alarm auto-report`** `{` *`module_name`* `[` *`group_name`* `] |` **`port-list`** *`port-list`* `] }` **`enable`**	Enable alarm auto-reporting.

Step	Command	Description
4	Qtech(config)#**alarm monitor** { *module_name* [*group_name*] | **port-list** *port-list* } **enable**	Enable alarm monitoring.
5	Qtech(config)#**alarm inverse port-list** *port-list* { **auto** | **manual** | **none** }	Configure alarm reverse mode.
6	Qtech(config)#**alarm** { **active** | **clear** } **delay** { *delay* }	Configure alarm delay.
7	Qtech(config)#**alarm active storage-mode** { **loop** | **stop** }	Configure alarm storage mode.
8	Qtech(config)#**alarm clear index** *index*	Clear current alarm of specified alarm index.
	Qtech(config)#**alarm clear** *module_name* [*group_name*]	Clear current alarm of specified feature module.
	Qtech(config)#**alarm clear port-list** *port-list*	Clear current alarm of specified feature module on a specified interface.
9	Qtech(config)#**alarm syslog enable**	Enable alarm to be output to system logs.
10	Qtech(config)#**exit** Qtech#**show alarm active** [*module_name* | **severity** *severity*]	Show current alarm information.
	Qtech#**show alarm cleared** [*module_name* | **severity** *severity*]	Show history alarm information.

Note

All modules providing alarm support can be configured to enable/disable alarm monitoring, alarm auto-reporting and alarm clear function.

10.9.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show alarm management** [*module_name*]	Show parameters of current alarms, including status of alarm inhibition, alarm reverse mode, alarm delay, and alarm storage mode, maximum alarm buffer size, and alarm log size.
2	Qtech#**show alarm log**	Show alarm statistics of system log.
3	Qtech#**show alarm management statistics**	Show statistics of alarm management module.

10.10 Hardware environment monitoring

10.10.1 Introduction

Hardware environment monitoring mainly refers to monitor the running environment of the QSW-8200 series switch. The monitoring alarm events include:

- Overtemperature alarms
- Overvoltage alarms
- Abnormal interface status alarms

There are several ways to notify the user when an alarm is generated. The alarm event output methods are as follows:

- Record device hardware environmental monitoring alarm buffer.
- Output Syslog.
- Send Trap to the NMS.

You can take measures accordingly to prevent failure when an alarm event occurs.

Alarm event

- Overtemperature alarm

The device is in support of overtemperature alarm event, when the current temperature is lower than low temperature threshold, the low temperature alarm event will generate. The QSW-8200 series switch supports saving the overtemperature alarm table, sending Trap to the NMS, and outputting to the system log.

When the device current temperature is higher than high temperature threshold, the high temperature alarm event will generate. The QSW-8200 series switch supports saving the device hardware environment monitoring alarm table, sending Trap to the NMS, and outputting to the system log.

- Overvoltage alarm

The device is in support of overvoltage alarm event, when the current voltage is lower than low voltage threshold, the low voltage alarm event will generate. The QSW-8200 series switch supports saving the overvoltage alarm table, sending Trap to the NMS, and outputting to the system log.

When current voltage value of the monitored voltage is greater than the threshold, a high voltage alarm is generated. The QSW-8200 series switch supports saving the overvoltage alarm table, sending Trap to the NMS, and outputting to the system log.

Note

The QSW-8200 series switch monitors 3.3 V master chip voltage only.

- Interface status anomaly alarm

Each interface has three alarm events:

  - Interface link-fault alarm: link failure alarm refers to the peer link signal loss. The alarm event only aims at optical interface, but not electrical interface.
  - Interface link-down alarm: interface status Down alarm.

- Interface not-forwarding alarm: The interface will change to non-forwarding state under all VLAN.

The QSW-8200 series switch supports saving the device hardware environment monitoring alarm table, sending Trap to the NMS, and outputting to the system log.

Alarm output mode

Hardware environment monitoring alarm output modes are as below.

- Hardware environment monitoring alarm buffer output, which is recorded to the hardware environment monitoring alarm table
  - The hardware environment monitoring alarm table, recording current alarm information which has not been cleared and restored.
  - The hardware environment monitoring history alarm table, recording current, restored and manually cleared alarm information.

Hardware environmental monitoring alarm information can be recorded in the current hardware environment monitoring alarm table and hardware environment monitoring history alarm table automatically without configuring manually.

- Trap output

Alarm information is output to the NMS in Trap mode.

Trap output has global switch and all monitored alarm events still have their own Trap output switches. When enabling the global switch and monitored alarm events switches simultaneously, the alarm will generate Trap output.

Table 10-5 lists Trap fields.

Table 10-5 Trap fields

Field	Description
Alarm status	• asserted (current alarm) • cleared (alarm recovery) • clearall (clear all alarm information)
Alarm source	• device (global alarm) • Interface number (interface status alarm)
Timestamp	Alarm time, in the form of absolute time
Alarm event type	• dev-power-down (power-down alarm) • power-abnormal (power-abnormal alarm, one of two powers is power down.) • high-temperature (high-temperature alarm) • low-temperature (low-temperature alarm) • high-volt (high-voltage alarm) • low-volt (low-voltage alarm) • link-down (interface LinkDown alarm) • not-forwarding (interface Not-Forwarding alarm) • link-fault (interface LinkFault alarm) • all-alarm (clear all alarm information)

- Syslog output

Record alarm information to Syslog.

Syslog output has global switch and all monitored alarm events still have their own Syslog alarm output switches. When the global switch and monitored alarm events switches are enabled concurrently, the alarm will generate Syslog.

Syslog contents are shown in Table 10-6.

Table 10-6 Syslog information

Field	Description
Facility	The module name generating alarm, the hardware environment monitoring module is fixed as alarm.
Severity	Level. See Table 10-2 for the same system log defined levels.
Mnemonics	Alarm event type. See Table 10-5 for the detailed type description.
Msg-body	Main body, describing alarm event contents.

10.10.2 Preparing for configurations

Scenario

Hardware environment monitoring provides environment monitoring function to the QSW-8200 series switch, by which you can monitor the fault. When the QSW-8200 series switch operation environment is abnormal, this function will record hardware environment monitoring alarm list, generate Syslog or send Trap and other alarm information to notify you to take corresponding measures and prevent fault.

Prerequisite

Hardware environment monitoring alarm output:

- In Syslog output mode, alarm information will generate system log. When you need to send alarm information to the system log host, configure the IP address of the system log host for the QSW-8200 series switch.
- In Trap output mode, configure the IP address of the NMS for the QSW-8200 series switch.

10.10.3 Default configurations of hardware environment monitoring

Default configurations of hardware environment monitoring are as below.

Function	Default value
Global hardware environment monitoring alarm Syslog output	Disable
Global hardware environment monitoring alarm Trap output	Disable
Power down event alarm	Enable Trap output. Enable Syslog output.
Temperature alarm output	

Function	Default value
Voltage alarm output	
Interface link-down event alarm output	
Interface link-fault event alarm	Disable Trap output. Disable Syslog output.
Interface not-forwarding event alarm output	
High temperature alarm threshold	60ºC
Low temperature alarm threshold	20ºC
High voltage threshold	3450 mV
Low voltage threshold	3150 mV

10.10.4 Enabling global hardware environment monitoring

Enable global hardware environment monitoring for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**logging alarm**	(Optional) enable global hardware environment monitoring alarm Syslog output.
3	Qtech(config)#**snmp-server alarm-trap enable**	(Optional) enable global hardware environment monitoring alarm Trap output.

Note

- When both alarm Syslog output for global hardware environment monitoring and Syslog output for alarm event are enabled, an alarm event can generate Syslog.
- When sending Trap for global hardware environment monitoring and Syslog output for alarm event are enabled, Trap will be sent when an alarm event is generated.

10.10.5 Configuring temperature monitoring alarm

Configure temperature monitoring alarm for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.

Step	Command	Description
2	Qtech(config)#**alarm temperature** { **high** *high-value* | **low** *low-value* | **notifies** | **syslog** }	Enable temperature alarm output and configure temperature alarm output mode or temperature alarm threshold. High temperature threshold *high-value* must be higher than low temperature threshold *low-value*. Low temperature threshold *low-value* must be lower than high temperature threshold *high-value*.

10.10.6 Configuring voltage monitoring alarm

Configure voltage monitoring alarm for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**alarm voltage** { **high** *high-value* | **low** *low-value* | **notifies** | **syslog** }	Enable voltage alarm output, and configure voltage alarm output mode or voltage alarm threshold. **Note** The QSW-8200 series switch monitors 3.3V master chip voltage only.

10.10.7 Configuring interface status monitoring alarm

Configure interface status monitoring alarm for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**alarm port** { **link-down** | **link-fault** | **not-forwarding** } { **notifies** | **syslog** } **port-list** *port-list*	Enable interface status alarm output and configure interface status alarm output mode.

10.10.8 Configuring polling period for environment monitoring

Configure the polling period for environment monitoring for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**alarm hwmonitor period** *period*	Configure the polling period for environment monitoring.

10.10.9 Clearing all hardware environments monitoring alarm event manually

Clear all hardware environments monitoring alarm event manually for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**clear alarm**	Clear alarms manually. **Note** Use this command to clear all alarms in current alarm list and generate an all-alarm alarm in history alarm list. If enabling global sending Trap, the all-alarm alarm will be output in Trap mode; if enabling global Syslog, the all-alarm alarm will be output in Syslog mode.

10.10.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show alarm**	Show global hardware environment monitoring alarm configuration. Use this command to check hardware environment monitoring information, including global alarm Syslog output, global sending Trap, power down alarm, temperature alarm and voltage alarm.
2	Qtech#**show alarm port-list** *port-list*	Show interface status alarm information.
3	Qtech#**show alarm currrent**	Show current alarm information about hardware environment monitoring.
4	Qtech#**show alarm history**	Show history alarm information about hardware environment monitoring.
5	Qtech#**show environment** [**power** | **temperature** | **voltage**]	Show the current power, temperature, voltage alarm and the current environment information.
6	Qtech#**show alarm hwmonitor period**	Show the polling period for hardware monitoring.

10.10.11 Example for configuring hardware environment monitoring

Networking requirements

As shown in, configure hardware environment monitoring function to monitor the QSW-8200 series switch temperature information. When the temperature exceeds threshold, alarm information will be output to the NMS in Trap mode. You will take corresponding measures to prevent fault.

Configuration steps

Step 1 Configure the IP address of the QSW-8200 series switch.

```
Qtech#config
Qtech(config)#interface ip 0
Qtech(config-ip)#ip address 20.0.0.6 255.255.255.0 1
Qtech(config-ip)#exit
```

Step 2 Configure the QSW-8200 series switch to send Trap.

```
Qtech(config)#snmp-server enable traps
Qtech(config)#snmp-server host 20.0.0.1 version 2c public
```

Step 3 Enable sending Trap for global hardware environment monitoring.

```
Qtech(config)#snmp-server alarm-trap enable
```

Step 4 Configure temperature monitoring for the QSW-8200 series switch.

```
Qtech(config)#alarm temperature notifies
Qtech(config)#alarm temperature high 50
Qtech(config)#alarm temperature low 20
```

Checking results

Use the **show snmp config** command to show configurations of sending Trap.

```
Qtech#show snmp config
SNMP trap status:    enable
SNMP engine ID:      0x006b7a303031666365383634376138
```

Use the **show snmp host** command to show configurations of the Trap target host.

```
Qtech#show snmp host
Index:        0
IP family:     IPv4
IP address:    20.0.0.1
Port:         162
User Name:     public
SNMP Version:   v2c
Security Level: noauthnopriv
TagList:       bridge config interface rmon snmp ospf
```

Use the **show alarm** command to show configurations of hardware monitoring alarm.

```
Qtech#show alarm
Traps alarm:                Enabled
Logging alarm:              Disabled
Temperature
   High threshold(Celsius):   50
   Low  threshold(Celsius):  20
   Notifies:               Enabled
   Syslog:                 Enabled
Voltage
   High threshold:          3450mV
   Low  threshold:          3150mV
   Notifies:               Disabled
  Syslog:                 Disabled
```

10.11 Fan monitoring

10.11.1 Introduction

The QSW-8200 series switch supports monitoring the fan, including the rotational speed and temperature. It sends Trap when the rotational speed or temperature is abnormal.

The QSW-8200 series switch monitors the fan in two modes:

- Forcible monitoring: forcibly set the rotational speed of the fan.
- Automatical monitoring: the fan adjusts its rotational speed by temperature.

In automatical monitoring mode, the rotational speed of the fan has four levels, and each of them corresponds to a temperature range. The fan adjusts its rotational speed by temperature.

10.11.2 Preparing for configurations

Scenario

In hot environment, over high temperature affects heat dissipation of the QSW-8200 series switch. Thus fan monitoring must be configured so that the fan speed is automatically adjusted according to environment temperature and the QSW-8200 series switch runs properly.

Precondition

N/A

10.11.3 Configuring fan monitoring

Configure fan monitoring for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`fan-monitor mode`** `{` **`auto`** `|` **`enforce`** `}`	Configure monitoring mode for the fan speed. By default, it is auto.
3	`Qtech(config)#`**`fan-monitor enforce level`** *`level`*	(Optional) configure the fan speed in enforced mode.
4	`Qtech(config)#`**`fan-monitor temperature-scale`** *`temperature1 temperature2 temperature3`*	(Optional) configure the temperature range for different fan speeds in automatical monitoring mode.
5	`Qtech(config)#`**`fan-monitor trap send enable`**	(Optional) configure fan alarm trap

10.11.4 Checking configurations

Use the following commands to check configuration results.

Step	Command	Description
1	`Qtech#`**`show fan-monitor information`**	Show fan monitoring configurations.
2	`Qtech#`**`show fan-monitor status`**	Show fan monitoring status.

10.12 CPU monitoring

10.12.1 Introduction

The QSW-8200 series switch supports CPU monitoring. It can monitor state, CPU utilization rate, and application of stacking of each task in real time in the system. It helps locate faults.

CPU monitoring can provide the following functions:

- Viewing CPU utilization rate

It can be used to view unitization of CPU in each period (5s, 1minute, 10minutes, 2hours). Total unitization of CPU in each period can be shown dynamically or statically.

It can be used to view the operational status of all tasks and the detailed running status information about assigned tasks.

It can be used to view history utilization of CPU in each period.

It can be used to view information about dead tasks.

- Threshold alarm of CPU unitization

If CPU utilization of the system is more than set upper threshold or less than preconfigured lower threshold in specified sampling period, Trap will be sent, and Trap will provide serial number of 5 tasks whose unitization rate of CPU is the highest in the latest period (5s, 1minute, 10minutes) and their CPU utilization rate.

10.12.2 Preparing for configurations

Scenario

CPU monitoring can give real-time monitoring to task state, CPU utilization rate and stack usage in the system, provide CPU utilization rate threshold alarm, detect and eliminate hidden dangers, or help administrator for fault location.

Prerequisite

When the CPU monitoring alarm information needs to be output in Trap mode, configure the Trap output target host address on the QSW-8200 series switch, which is the IP address of the NMS server.

10.12.3 Default configurations of CPU monitoring

Default configurations of CPU monitoring are as below.

Function	Default value
CPU utilization rate alarm Trap output	Disable
Upper threshold of CPU utilization rate alarm	100%
Lower threshold of CPU utilization rate alarm	1%
Sampling period of CPU utilization rate	60s

10.12.4 Checking CPU monitoring information

Configure CPU monitoring information about the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`show cpu-utilization`** `[` **`dynamic`** `|` **`history`** `{` **`10min`** `|` **`1min`** `|` **`2hour`** `|` **`5sec`** `} ]`	Show CPU utilization rate.
2	`Qtech#`**`show process`** `[` **`dead`** `|` **`sorted`** `{` **`normal-priority`** `|` **`process-name`** `} |` *`taskname`* `]`	Show task status.
3	`Qtech#`**`show process cpu`** `[` **`sorted`** `[` **`10min`** `|` **`1min`** `|` **`5sec`** `|` **`invoked`** `] ]`	Show CPU utilization rate of all tasks.

10.12.5 Configuring CPU monitoring alarm

Configure CPU monitoring alarm for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`snmp-server traps enable cpu-threshold`**	Enable sending Trap for CPU threshold.
3	`Qtech(config)#`**`cpu rising-threshold`** *`rising-threshold-value`* `[` **`falling-threshold`** *`falling-threshold-value`* `]` `[` **`interval`** *`interval-value`* `]`	(Optional) configure the upper CPU threshold and lower CPU threshold. The upper CPU threshold must be greater than the lower CPU threshold. After CPU threshold Trap is enabled, in the sampling interval, when the CPU utilization rate is higher than the upper CPU threshold or is smaller than the lower CPU threshold, a Trap alarm message will be sent automatically.

10.12.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Qtech#`**`show cpu-utilization`** `{` **`dynamic`** `|` **`history`** `{` **`10min`** `|` **`1min`** `|` **`2hour`** `|` **`5sec`** `} }`	Show CPU utilization and configurations.

10.13 Caching CPU packets

10.13.1 Introduction

Caching CPU packet makes a copy of packets to CPU on the designated interface and saves them in a buffer. You can enable this feature for analysis and statistics. This feature will not affect the packets forwarding on the QSW-8200 series switch, and will buffer the packets at the same time for user analysis.

Not all the packets should be sent to the CPU for process, only the packets to the CPU will be cached. If you wish to cache all the traffic, port mirroring is needed as well. There are two kinds of mirror functions to mirror packets to the CPU.

- Port mirroring: configure the monitor interface as the CPU. Packets matching mirroring rule on the mirroring port will be cached.
- Flow mirror: configure a traffic policy with action **copy-to-mirror** by sending a certain kind of traffic to CPU. In this way, the CPU has less load and cached packets are uniform in type. It is easier for you to analyze traffic.

For better traffic monitor, caching CPU packets provides the command used with ACL rules. ACL will filter the traffic and help you buffer packets that you are interested in.

Packet overwriting modes

In the buffer, packets are stored in rewritable and non-rewritable modes:

- Rewritable: when the buffer is full, new arrival packets can overwrite the oldest packets. Hence, the buffer always stores the latest packets. You can check traffic during the last period of time.
- Non-rewritable: when the buffer is full, new arrival packets will be discarded. You can check traffic of a certain time.

Packet checking modes

There are two modes for you to check the cached packets. You can use either or both of them at the same time.

- Using command to check the packets through the Console interface of the Switch.
  - Check the summary of cached packets.
  - Check the detail information about cached packets.
  - Check packets statistics according to protocol type or MAC address.
- Upload packets to the remote server

You can use FTP or TFTP. FTP or TFTP server software is needed on the remote server device and allows the server to create or rewrite a file. Packets are grouped and saved in the form of pcap file. You can view contents of packets with packet capturing software.

Packet upload

There are three upload methods:

- Auto upload

The upload times are preconfigured. When the buffer is full of packets, the QSW-8200 series switch will upload cached packets to the specified remote server without any user operation.

- Manually upload

Any time you wish to upload the current packets in the buffer to the server, you can use this command to upload packets in the current buffer.

- No upload

When the buffer is full, the QSW-8200 series switch will not upload any file to the remote server, but continue buffering the packets.

10.13.2 Preparing for configurations

Scenario

CPU packet caching provides you to view the data being exchanged inside the Switch at any time, and helps you locate the root cause to unexpected situations. This feature mainly monitors packets to the CPU or matches some ACL rules. It is greatly helpful when analyzing big suspicious traffic.

Prerequisite

N/A

10.13.3 Default configurations of caching CPU packets

Default configurations of caching CPU packets are as below.

Function	Default value
CPU packet caching	Disable
Filtering caching packets	Disable
Buffer size	512 KBytes
Upload method	No upload
Overwrite mode	Rewritable
Length of cached packet	First 64 Bytes of packets
Mirror to the CPU	Disable

10.13.4 Configuring caching CPU packets

⚠Caution

- If packets on an interface are mirrored to the CPU, the CPU will have to endure a large pressure. We do not recommend you to configure port mirroring of which the mirroring ports are all interfaces and the monitor port is the CPU.
- We do not recommend configuring the upload times as infinite.

Configure caching CPU packets QSW-8200 series switch as below:

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**cache packet** [**port-list** *port-list*]	Enable CPU cache function.
3	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
4	Qtech(config-port)#**cache packet access-list** { **access-list-map** | **ip-access-list** | **mac-access-list** } *acl-number* Qtech(config-port)#**exit**	(Optional) configure rules for caching packets on the interface, and return to global configuration mode.
5	Qtech(config)#**cache packet length** { **all** | **header** }	(Optional) configure length of cached packets.
6	Qtech(config)#**cache packet buffer-size** *size*	(Optional) configure size of buffer.
7	Qtech(config)#**cache packet buffer** { **override** [**auto-upload** { **times** *times* | **infinite** }] | **nooverride** [**auto-upload**] }	(Optional) configure overwrite mode and upload method.
8	Qtech(config)#**cache packet upload-server** { **ftp** *ip-address user-name password* | **tftp** *ip-address* }	(Optional) configure the upload server.
9	Qtech(config)#**cache packet upload** [**clear-cache**]	(Optional) enable automatical uploading of cached packets.
10	Qtech(config)#**cache packet outband**	(Optional) enable the function of copying packets to be sent to the CPU to the out-of-band management interface.

10.13.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show cache packet** [**interface** | **port** *port-id*]	Show configurations of caching CPU packets.
2	Qtech#**show cache packet summary order** [**start-order** *order* **counter** *counter*]	Show summary of cache packet by index.
	Qtech#**show cache packet summary time from** *hour minute second* [*interval*]	Show summary of cache packet by time sequence.
	Qtech#**show cache packet summary time last** *past-seconds*	

No.	Command	Description
3	`Qtech#`**`show cache packet statistics`** `{` **`mac`** `|` **`protocol`** `}` `{` **`global`** `|` **`port`** *`port-id`* `|` **`vlan`** *`vlan-id`* `}`	Show statistics of cache packets
4	`Qtech#`**`show cache packet detail`** *`order`*	Show details of packets on a specified number in the cache.

10.13.6 Maintenance

Maintain the QSW-8200 series switch as below.

Command	Description
`Rasiecom(config)#`**`clear cache packet buffer`**	Clear cached packets.

10.13.7 Example for configuring caching CPU packets

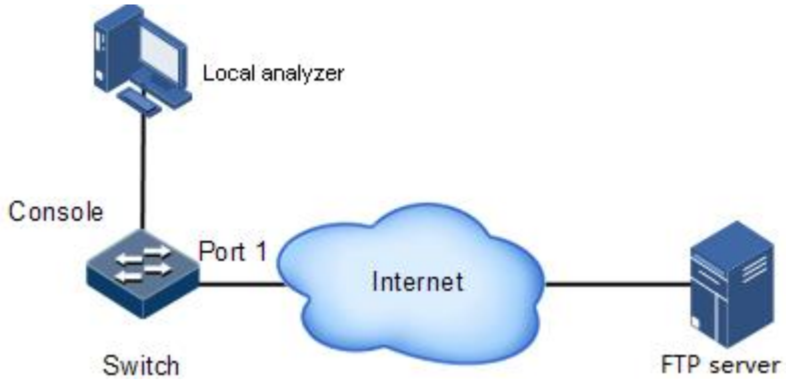
Networking requirements

As shown in Figure 10-11, the local analyzer is connected to console on the Switch, checking cache packets. The switch uploads cached packets to remote server for future analysis.

Combining with interface mirror, buffer all the non-IP type traffic on Port 1, and requirement are as below:

- Upload traffic through FTP. The IP address of the FTP server is 192.168.10.10/255.255.255.0, the user name is Qtech, and the password is 123456.
- Overwrite mode is Rewritable, and the auto upload times is 10.
- Enable caching CPU packets on the interface.
- Configure filter based on IP ACL. The ACL rule is to deny all IP packets from passing.
- Enable interface mirror to mirror packets to the CPU.

Figure 10-11 Caching CPU packet networking



Configuration steps

Step 1 Configure the remote server.

```
Qtech#config
Qtech(config)#cache packet upload-server ftp 192.168.10.10 Qtech 123456
```

Step 2 Configure packets uploading method as auto.

```
Qtech(config)#cache packet buffer override auto-upload times 10
```

Step 3 Enable interface cache.

```
Qtech(config)#cache packet port-list 1
```

Step 4 Configure cache filtering rule.

```
Qtech(config)#ip-access-list 0 deny ip any any
Qtech(config)#interface port 1
Qtech(config-port)#cache packet access-list ip-access-list 0
Qtech(config-port)#exit
```

Step 5 Enable port mirroring of traffic to the CPU.

```
Qtech(config)#mirror enable
Qtech(config)#mirror monitor-cpu
Qtech(config)#mirror source-port-list ingress port-list 1
```

Checking results

Use the **show cache packet** command to show configurations of caching CPU packets.

```
Qtech#show cache packet
ccp               : enable
portlist          : port-list 1
buffer-size        : 512KB
buffer-mode        : override
buffer-status      : not full
packet-length      : 64B
upload-mode        : auto-upload
auto-upload times  : 10
uploaded count     : 0
```

```
curent-status      : no action
pkt-count          : 0
uploaded pkt number: 0
server              : enable
upload-protocol     : ftp
    ip-address      : 192.168.11.107
    username         : Qtech
    Password         : 123456
```

10.14 Dual systems

10.14.1 Introduction

The dual systems function refers to that the Flash saves two versions of system software. You can choose one to run the QSW-8200 series switch.

The dual-system device can meet users' diverse requirements:

- Upgrade system software through: to upgrade the system to a new version, you can download the new version to the Flash, set it as the startup file for software upgrade.
- Choose different systems to run at different periods: you can save different versions of system software in the Flash, and choose different system to run at different periods through simple operation.
- System security: to remotely manage the QSW-8200 series switch, you can start the QSW-8200 series switch from the other version without going on site if one version is corrupted.

The dual-system device is more flexible and convenient for your applications.

10.14.2 Configuring dual systems

Configure dual systems for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**multisystem select**	Configure system startup list.
2	Qtech#**show multisystem**	Show information about the system startup file.

10.15 Auto-Provisioning

10.15.1 Introduction

As Information Technology (IT) grows rapidly, enlargement of the IT network results in high complexity of configuring devices. A large number of network devices bring much workload for the network administrator. In addition, the wide distribution of network devices adds difficulty to the on-site deployment and maintenance. As a result, Auto-Provisioning is introduced to make the entire network more effectively running and to uniformly configure management policies.

The Auto-Provisioning function of the QSW-8200 series switch involves two device roles and a channel: the CO device, remote device, and the management channel. By making SNMP transmit Advertise packets, which carry information about configuring the remote device such as the IP address and VLAN, Auto-Provisioning transmits management information to the remote device so that the remote device can be automatically configured upon access to the network.

10.15.2 Preparing for configurations

Scenario

After configured with Auto-Provisioning, the CO device can automatically deploy remote devices without any configurations. Meanwhile the CO device records information about the remote device.

Precondition

N/A

10.15.3 Default configurations of Auto-Provisioning

Default configurations of Auto-Provisioning on the CO device are as below.

Function	Default value
Mode for forwarding packets by the remote device	Terminate
Interval for sending packets	5s
Whether to generate static ARP entries of the CO	No
Auto-Provisioning on the remote device	Enable
Management network segment	10
List of interfaces for sending packets	Member interfaces of the management VLAN
Trap	Disable

10.15.4 Configuring management VLAN on CO device

Configure the management VLAN on the CO device for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`interface ip`** *`if-interface`*	Enter Layer 3 interface configuration mode.

Step	Command	Description
3	`Qtech(config-ip)#`**`ip vlan`** *`vlan-id`*	Configure the management VLAN on the IP interface.

10.15.5 Configuring management network segment on CO device

Configure the management network segment on the CO device for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`interface ip`** *`if-number`*	Enter Layer 3 interface configuration mode.
3	`Qtech(config-ip)#`**`auto-provision network`** *`network`*	Configure the management network segment of the IP interface.

10.15.6 Configuring interface list on CO device

Configure the interface list on the CO device for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`interface ip`** *`if-number`*	Enter Layer 3 interface configuration mode.
3	`Qtech(config-ip)#`**`auto-provision port-list`** *`port-list`*	Configure Auto-Provisioning interface list on the IP interface.

10.15.7 Configuring IP address of SNMP server

Configure the IP address of the SNMP server for the QSW-8200 series switch as below.

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`interface ip`** *`if-number`*	Enter Layer 3 interface configuration mode.
3	`Qtech(config-ip)#`**`auto-provision snmp-host`** *`ip-address`*	Configure the IP address of the Auto-Provisioning SNMP server.

10.15.8 Configuring IP address of TFTP server

Configure the IP address of the TFTP server for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface ip** *if-number*	Enter Layer 3 interface configuration mode.
3	Qtech(config-ip)#**auto-provision tftp-server** *ip-address*	Configure the IP address of the Auto-Provisioning TFTP server.

10.15.9 Configuring rules for configuration file

Configure rules for the configuration file for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface ip** *if-number*	Enter Layer 3 interface configuration mode.
3	Qtech(config-ip)#**auto-provision filename** [**rule** *rule-number* [**prefix** *prefix*] [**postfix** *postfi*x]]	Configure rules, prefix, and suffix of the name of Auto-Provisioning configuration file.

10.15.10 Enabling Auto-Provisioning on CO device

Enable Auto-Provisioning on the CO device for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface ip** *ip-number*	Enter Layer 3 interface configuration mode.
3	Qtech(config-ip)#**auto-provision advertise interval** *interval*	Configure the interval for sending messages in Auto-Provisioning.
5	Qtech(config-ip)#**ip auto-provision** { **times** *times* | **forever** }	Configure the times of sending messages in Auto-Provisioning, and enable Auto-Provisioning on the CO device.
6	Qtech(config-ip)#**ip auto-provision stop**	Stop the CO device to send Auto-Provisioning packets.

Note

In Layer 3 interface configuration mode, use the **no ip auto-provision** command to disable Auto-Provisioning and clear remote device information.

10.15.11 Configuring remote device to generate ARP entries

Configure the remote device to generate ARP entries as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface ip** *if-number*	Enter Layer 3 interface configuration mode.
3	Qtech(config-ip)#**auto-provision arp generation**	Configure the remote device to generate ARP entries.

10.15.12 Enabling Auto-Provisioning for remote device

Enable Auto-Provisioning for the remote device on the CO device as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**auto-provision client enable**	Auto-Provisioning for the remote device on the CO device.

Note

By receiving the Advertise packet from the CO device, a remote device creates VLANs according to VLAN TLV carried in the Advertise packet, and then adds the interface that receives the Advertise packet into the VLAN. If the VLAN is manually modified or is the default VLAN, Auto-Provisioning will fail.

10.15.13 Configuring mode for forwarding packets by remote device

Configure the mode for forwarding packets by remote device as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**auto-provision advertise** { **forward** | **terminal** }	Configure the mode for forwarding packets by remote device.

10.15.14 (Optional) enabling sending Trap

Enable sending Trap for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.

Step	Command	Description
2	Qtech(config)#**interface ip** *if-number*	Enter Layer 3 interface configuration mode.
3	Qtech(config-ip)#**auto-provision send trap enable**	Enable sending Trap for Auto-Provisioning.

10.15.15 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show auto-provision status** [*if-number*]	Show Auto-Provisioning configurations of the IP interface on the CO device.
2	Qtech#**show auto-provision remote-device** [*if-number*] [*mac-address*]	Show remote device information recorded on the CO device.
3	Qtech#**show auto-provision client**	Show configurations and current status of the remote device.

10.15.16 Maintenance

Maintain the QSW-8200 series switch as below.

Command	Description
Qtech(config)#**clear auto-provision statistics** *if-number*	Clear statistics of packets on the IP interface on the CO device.
Qtech(config)#**clear auto-provision statistics client**	Clear statistics of packets on the CO device.
Qtech(config)#**clear auto-provision statistics client**	Clear message statistics on the IP interface on the remote device.

10.15.17 Example for configuring Auto-Provisioning

Networking requirements

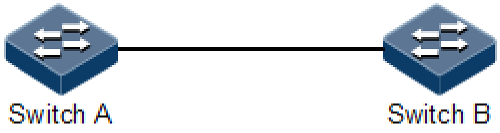
As shown in Figure 10-12, Switch A, as the CO device, manages the remote Switch B through Auto-Provisioning so that Switch B can be automatically configured upon being powered on.

Configure parameters as below:

- The management network segment for IP interface 1 is 12.
- The IP address of the SNMP server is 12.3.3.3.

- The interface list for sending Auto-Provisioning packets is port 1.
- The interval for sending packets is 10s, the sending times are 10, and the management VLAN ID is 16.
- Generate static ARP entries for Switch A, and discard Auto-Provisioning packets.
- Enable sending Trap for Auto-Provisioning.

Figure 10-12 Auto-Provisioning networking



Configuration steps

Configure Switch A.

Step 1 Configure the management VLAN ID of IP interface 1 as 16, and activate VLAN 16.

```
Qtech#hostname SwitchA
SwitchA#config
SwitchA(config)#interface ip 1
SwitchA(config-ip)#ip vlan 16
SwitchA(config-ip)#exit
SwitchA(config)#create vlan 16 active
```

Step 2 Set the interface connected to Switch B in Trunk mode.

```
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport mode trunk
```

Step 3 Configure the management network segment of IP interface 1 as 12.

```
SwitchA#config
SwitchA(config)#interface ip 1
SwitchA(config-ip)#auto-provision network 12
```

Step 4 Set the IP address of the SNMP server to 12.3.3.3.

```
SwitchA(config-ip)#auto-provision snmp-host 12.3.3.3
```

Step 5 Configure the interface list for sending Auto-Provisioning packets.

```
SwitchA(config-ip)#auto-provision port-list 1
```

Step 6 Enable sending Trap for Auto-Provisioning.

```
SwitchA(config-ip)#auto-provision send trap enable
```

Step 7 Configure Switch B to generate static ARP entries for Switch A.

```
SwitchA(config-ip)#auto-provision arp generation
```

Step 8 Set the internal for sending Auto-Provisioning packets to 10s, and sending times to 10.

```
SwitchA(config-ip)#auto-provision advertise interval 10
SwitchA(config-ip)#ip auto-provision times 10
SwitchA(config-ip)#exit
```

Step 9 Enable Auto-Provisioning on Switch B.

```
SwitchA(config)#auto-provision client enable
```

Step 10 Configure Switch B to discard Auto-Provisioning packets.

```
SwitchA(config)#auto-provision advertise terminal
```

Configure Switch B.

Step 11 Set the Switch B interface connected to Switch A in Trunk mode.

```
Qtech#config
Qtech(config)#interface port 1
Qtech(config-port)#switchport mode trunk
```

Checking results

Use the **show auto-provision status** command to show configurations of Auto-Provisioning.

```
SwitchA#show auto-provision status
```

```
IP interface 0
Network segment: 10
Port list: --
Interval: 5
Times: --
ARP Generated: NO
SNMP host:--
Auto provision status: CLOSED
Send Trap: NO
Sequence: 0
Times of sending Advertise: 0
Times of receiving ACK: 0

IP interface 1
Network segment: 12
Port list: port-list 1
Interval: 10
Times: 10
ARP Generated: YES
SNMP host:12.3.3.3
Auto provision status: OPEN
Send Trap: YES
Sequence: 1
Times of sending Advertise: 10
Times of receiving ACK: 3
……
```

Use the **show auto-provision remote-device** command to show remote device information recorded on the CO device.

```
SwitchA#show auto-provision remote-device
MAC         IP interface      IP Address       Type        Port    Status
Vid
-------------------------------------------------------------------------
-----
001F.CE00.000A      1        12.0.0.10  QSW-8200/D  3        OK
16
```

Use the **show auto-provision client** command to show configurations and current status of the remote device.

```
SwitchA#show auto-provision client
Terminal Advertise: Terminal
Remote Device Function: Disable
Network segment: 12
SNMP host:  12.3.3.3
Sequence: 1
Generate ARP: YES
Vlan id: 16
Port:  1
Management Status: YES
```

```
Times of processing Advertise: 3
Times of discarding Advertise: 7
Times of reponsing Advertise: 3
```

10.16 Checking device information

Check device information about the QSW-8200 series switch as below.

No.	Command	Description
1	Qtech#**show version**	Show the device version.
2	Qtech#**show running-config**	Show the current configuration file.
3	Qtech#**show clock**	Show the system time.
4	Qtech#**show environment** [**power** | **temperature** | **voltage**]	Show the current power, temperature, and voltage.
5	Qtech#**show power-card**	Show the power type and serial No.
6	Qtech#**show memory** [**detail**]	Show memory usage.

10.17 Memory management

Configure memory management for the QSW-8200 series switch as below.

No.	Command	Description
1	Qtech#**show memory** [**detail**]	Show memory usage.
2	Qtech#**show memory address** *address*	Show memory information.
3	Qtech#**show memory instruct** *instruct*	Show instruct address information about assigned memory.
4	Qtech#**show memory module** [*module*]	Show information about memory in use.
5	Qtech#**show memory summary** [*module*]	Show information about memory that is assigned but not released.
6	Qtech#**config** Qtech(config)#**reserved-memory-free**	Release reserved memory.

10.18 Loopback

10.18.1 Introduction

Loopback function will match the traffic using rules configured by user, and return the matched packets from receiving interface to sender at peer end. The peer end device can examine the network communication status by comparing the sent packets and returned packets.

Loopback mode involves layer 1 loopback and layer 2 loopback.

- Layer 1 loopback will return all the received traffic on an enabled interface back. This is used in layer 1 network.
- Layer 2 loopback is based on source MAC, packet protocol type and VLAN. A layer 2 loopback enabled device will match the packets using configured rules, exchange the source and destination MAC of these packets and send them back from the Rx interface. Not all the traffic will be returned. This function is used in testing link communication status when there is no Ethernet Private Line (EPL) service link.

Loopback rules:

- Layer 1 loopback: when it is enabled on interface, all the traffic received on this interface will be returned back without changing.
- Layer 2 loopback: when it is enabled on interface and configure loopback rule(source MAC, protocol type and VLAN), all the matched traffic received on this interface will be returned back.

Figure 10-14 shows loopback networking. Enable loopback on port 1 on Switch A and configure loopback rule. Switch B sends packets to port 1 on Switch A. Switch A will send the packet matching configured loopback rule back to Switch B from port 1. On Switch B, you can compare the sent and received packets, and thus check network communication status.

Figure 10-13 Layer 1 loopback networking

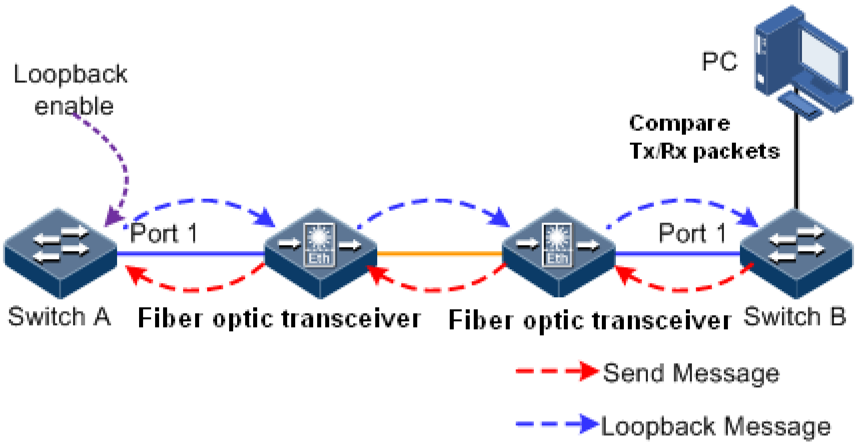
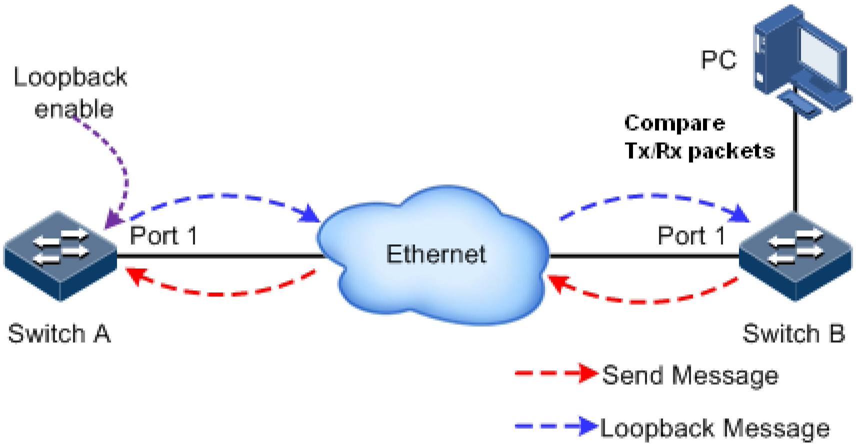


Figure 10-14 Layer 2 loopback networking



10.18.2 Preparing for configurations

Scenario

Through the loopback function, you can configure interface loopback rules and parameters so that received packets matching rules could be sent back to the peer end. Then, you can examine the network communication status.

Precondition

N/A

10.18.3 Default configurations of Loopback

Default configurations of loopback are as below.

Function	Default value
Loopback mode	l1 (Layer 1 loopback)
Loopback status	Disable

10.18.4 Configuring loopback rule

Configure loopback rule for the QSW-8200 series switch as below:

Step	Command	Description
1	`Qtech#`**`config`**	Enter global configuration mode.
2	`Qtech(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Qtech(config-port)#`**`loopback mode`** `{` **`l1`** `|` **`l2`** `}`	Configure Loopback mode.

Step	Command	Description
4	Qtech(config-port)#**loopback rule smac** *mac-address* [**ethertype** *number*] [**vlan** *vlan-id*]	Configure loopback mode.
5	Qtech(config-port)#**loopback l2-rule** *rule-id* **smac** *mac-address* [**ethertype** *number*] [**vlan** *vlan-id*]	(Optional) configure Loopback rule The source MAC is forbidden to set as multicast, broadcast or address of the QSW-8200 series switch.
5	Qtech(config-port)# **loopback l3-rule** *rule-id ip address* **[dscp** *value***] mac** *mac-address* **svla***n vlan-id* [**cvlan** *vlan id*]	(Optional) configure Layer 3 loopback rules. The source MAC address cannot be set as the multicast address, broadcast address, or MAC address of the QSW-8200 series switch.

10.18.5 Enabling loopback rule

Enable loopback rule for the QSW-8200 series switch as below:

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Qtech(config-port)#**loopback enable**	Enable the loopback function.

10.18.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Qtech#**show loopback** [**port-list** *port-list*]	Show loopback configurations.
2	Qtech#**show loopback statistics** [**port-list** *port-list*]	Show statistics of loopback packets.

10.18.7 Maintenance

Maintain the QSW-8200 series switch as below.

Command	Description
Qtech(config)#**clear loopback statistics** [**port-list** *port-list*]	Clear statistics of loopback packets on the interface.

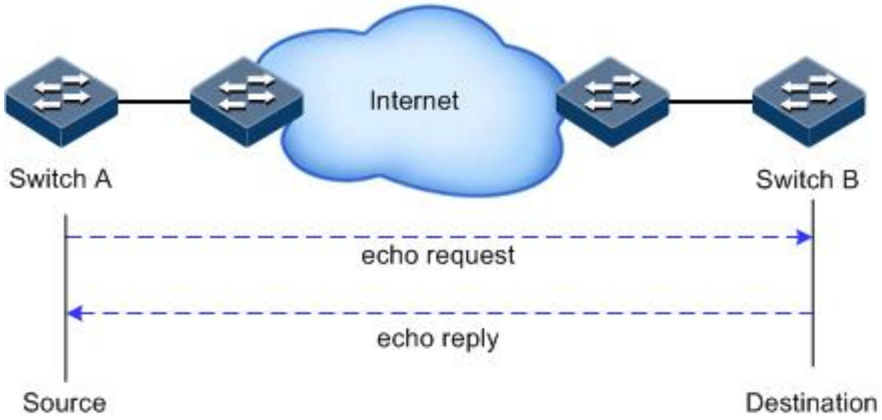
10.19 Ping

10.19.1 Introduction

Ping derives from the sonar location operation, which is used to detect whether the network is normally connected. Ping is achieved with ICMP echo packets. If an Echo Reply packet is sent back to the source address during a valid period after the Echo Request packet is sent to the destination address, it indicates that the route between source and destination address is reachable. If no Echo Reply packet is received during a valid period and timeout information is displayed on the sender, it indicates that the route between source and destination addresses is unreachable.

Figure 10-15 shows the principle of Ping.

Figure 10-15 Principle of Ping



10.19.2 Configuring Ping

Configure Ping for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**ping** *ip-address* [**count** *count*] [**size** *size*] [**waittime** *period*]	(Optional) use the **ping** command to test connectivity of the IPv4 network.
2	Qtech#**ping ipv6** *ipv6-address* [**count** *count*] [**size** *size*] [**waittime** *period*]	(Optional) use the **ping** command to test connectivity of the IPv6 network.

Note

The QSW-8200 series switch cannot perform other operations in the process of Ping. It can perform other operations only when Ping is complete or break off through **Ctrl**+**C**.

10.20 Traceroute

10.20.1 Introduction

Just as Ping, Traceroute is a commonly-used maintenance method in network management. Traceroute is often used to test the network nodes of packets from sender to destination, detect whether the network connection is reachable, and analyze network fault

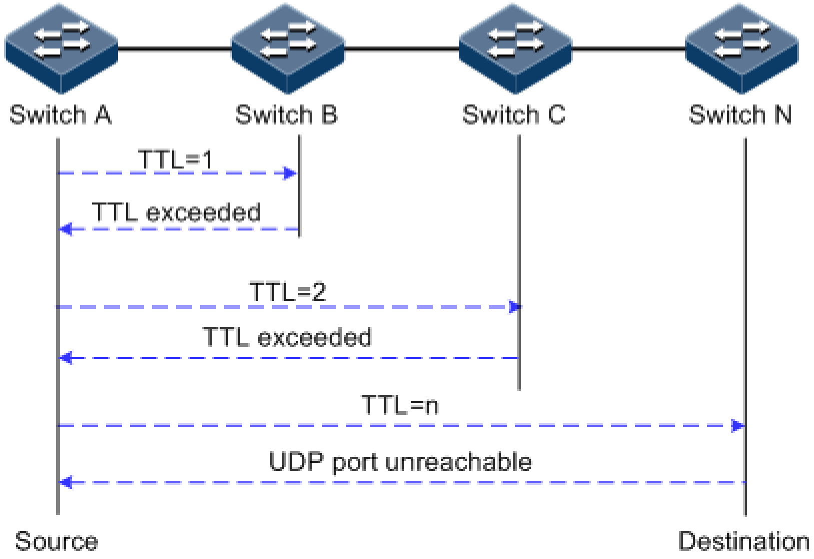
The following shows how Traceroute works:

- First, send a piece of TTL1 sniffer packet (where the UDP port ID of the packet is unavailable to any application programs in destination side).
- TTL deducts 1 when reaching the first hop. Because the TTL value is 0, in the first hop the device returns an ICMP timeout packet, indicating that this packet cannot be sent.
- The sending host adds 1 to TTL and resends this packet.
- Because the TTL value is reduced to 0 in the second hop, the device will return an ICMP timeout packet, indicating that this packet cannot be sent.

The previous steps continue until the packet reaches the destination host, which will not return ICMP timeout packets. Because the port ID of destination host is not be used, the destination host will send the port unreachable packet and finish the test. Thus, the sending host can record the source address of each ICMP TTL timeout packet and analyze the path to the destination according to the response packet.

Figure 10-16 shows the principle of traceroute.

Figure 10-16 Principle of Traceroute



10.20.2 Configuring Traceroute

Configure the IP address and default gateway for the QSW-8200 series switch before using Traceroute function.

Configure Traceroute for the QSW-8200 series switch as below.

Step	Command	Description
1	Qtech#**config**	Enter global configuration mode.
2	Qtech(config)#**interface ip** *if-number*	Enter Layer 3 interface configuration mode.
3	Qtech(config-ip)#**ip address** *ip-address* [*ip-mask*] *vlan-id*	Configure interface IP address.
4	Qtech(config-ip)#**exit**	Exit interface configuration mode and Enter global configuration mode.
5	Qtech(config)#**ip default-gateway** *ip-address*	Configure default gateway.
6	Qtech(config)#**exit**	Exit global configuration mode and enter privileged EXEC mode.
7	Qtech#**traceroute** *ip-address* [**firstttl** *first-ttl*] [**maxttl** *max-ttl*] [**port** *port-id*] [**waittime** *second*] [**count** *times*]	(Optional) test IPv4 network connection by traceroute and check packet passed network nodes.
8	Qtech#**traceroute ipv6** *ipv6-address* [**firstttl** *first-ttl*] [**maxttl** *max-ttl*] [**port** *port-id*] [**waittime** *second*] [**count** *times*]	(Optional) test IPv6 network connection by traceroute and check packet passed network nodes.

11 Appendix

This chapter lists terms, acronyms, and abbreviations involved in this document, including the following sections:

- Terms
- Acronyms and abbreviations

11.1 Terms

802.1Q in 802.1Q

The technique is also known as Stacked VLANs or Double VLAN. Just as QinQ extends 802.1Q, QinQ itself is extended by other Metro Ethernet protocols. Basic QinQ is a simple Layer 2 VPN tunnel technology that encapsulate outer VLAN Tag for subscriber's private packet at carrier's access end, then the packet take two layers of VLAN Tag to transport through the backbone network (public network) of the carrier. In public network, packet only be transmitted according to outer VLAN Tag (the public VLAN Tag); subscriber's private VLAN Tag is taken as part of data in the packet for transmission.

C

Connectivity Fault Management (CFM)

Ethernet CFM protocol is a kind of end-to-end service level OAM protocol to help administrators debug Ethernet Virtual Connection (EVC). It helps reducing network maintenance cost by using fault management function and improving maintenance of Ethernet.

E

Ethernet Ring Protection Switching (ERPS)

ERPS is an effort at ITU-T under G.8032 Recommendation to provide Automatic Protection and recovery switching for Ethernet traffic in a ring topology and at the same time ensuring that there are no loops formed at the Ethernet layer. When there is fault in link or device, the service can quickly switch to standby link and ensure service recovery soon.

Ethernet Linear Protection Switching (ELPS)

ELPS is an effort at ITU-T under G.8031 recommendation to provide Automatic Protection Switching protocol to protect an Ethernet link. It is a kind of end-to-end protection technology, including linear 1+1 protection switching and 1:1 protection switching.

L

Link Aggregation

Within the IEEE specification the Link Aggregation Control Protocol (LACP) provides a method to control the bundling of several physical ports together to form a single logical channel. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that also implements LACP).

11.2 Acronyms and abbreviations

A

ACL	Access Control List
APS	Automatic Protection Switching

C

CCM	Continuity Check Packet
CFM	Connectivity Fault Management
CoS	Class of Service

D

DoS	Deny of Service
DRR	Deficit Round Robin
DSCP	Differentiated Services Code Point

E

EFM	Ethernet in the First Mile
ELPS	Ethernet Linear Protection Switching
ERPS	Ethernet Ring Protection Switching
EVC	Ethernet Virtual Connection

F

FTP	File Transfer Protocol

G

GARP	Generic Attribute Registration Protocol
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GVRP	GARP VLAN Registration Protocol

I

IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITU-T	International Telecommunications Union - Telecommunication Standardization Sector

L

LACP	Link Aggregation Control Protocol
LBM	LoopBack Packet
LBR	LoopBack Reply
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit
LTM	LinkTrace Packet
LTR	LinkTrace Reply

M

MA	Maintenance Association
MAC	Medium Access Control
MD	Maintenance Domain
MEG	Maintenance Entity Group
MEP	Maintenance associations End Point
MIB	Management Information Base
MIP	Maintenance association Intermediate Point
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol

N

NNM	Network Node Management

O

OAM	Operation, Administration, and Management

P

PC	Personal Computer

Q

QoS	Quality of Service

R

RADIUS	Remote Authentication Dial In User Service
RMON	Remote Network Monitoring
RMEP	Remote Maintenance association End Point
RNC	Radio Network Controller
RSTP	Rapid Spanning Tree Protocol

S

SFP	Small Form-factor Pluggable
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SP	Strict-Priority
SSHv2	Secure Shell v2
STP	Spanning Tree Protocol

T

TACACS+	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLV	Type, Length, and Value
ToS	Type of Service

V

VLAN	Virtual Local Area Network

W

WRR	Weight Round Robin