

System Configuration

System Configuration

1. CONFIGURING CLI	1-1
1.1. Overview	1-1
1.2. Applications	1-1
1.2.1. Configuring and Managing Network Devices Through CLI	1-1
1.3. Features	1-2
1.3.1. Accessing CLI	1-2
1.3.2. Command Modes	1-3
1.3.3. System Help.	1-4
1.3.4. Abbreviated Commands	1-6
1.3.5. No and Default Options of Commands	1-7
1.3.6. Prompts Indicating Incorrect Commands	1-7
1.3.7. History Commands	1-7
1.3.8. Featured Editing	1-8
1.3.9. Searching and Filtering of the Show Command Output	1-9
1.3.10. Command Alias	1-10
2. CONFIGURING BASIC MANAGEMENT	2-1
2.1. Overview	2-1
2.2. Applications	2-1
2.2.1. Network Device Management	2-1
2.3. Features	2-1
2.3.1. User Access Control	2-3
2.3.2. Login Authentication Control	2-4
2.3.3. Basic System Parameters	2-6
2.3.4. Displaying Configurations	2-8
2.3.5. Configuration Rollback	2-8
2.3.6. Telnet	2-9
2.3.7. Restart	2-10
2.4. Configuration	2-11
2.4.1. Configuring Passwords and Privileges	2-12
2.4.2. Configuring Login and Authentication	2-17
2.4.3. Configuring Basic System Parameters	2-23
2.4.4. Enabling and Disabling a Specific Service	2-28
2.4.5. Rolling Back System Configurations	2-28
2.4.6. Configuring a Restart Policy	2-30
2.5. Monitoring	2-31

3. CONFIGURING LINES	3-1
3.1. Overview	3-1
3.2. Applications	3-1
3.3.1. Accessing a Device Through Console	3-1
3.3.1. Accessing a Device Through VTU	3-1
3.3. Features	3-2
3.3.1. Basic Features	3-2
3.4. Configuration	3-3
3.4.1. Entering Line Configuration Mode	3-3
3.5. Monitoring	3-7
4. CONFIGURING TIME RANGE	4-1
4.1. Overview	4-1
4.2. Typical Application	4-1
4.2.1. Applying Time Range to an ACL	4-1
4.3. Function Details	4-2
4.3.1. Using Absolute Time Range	4-2
4.3.2. Using Periodic Time	4-3
4.4. Configuration Details	4-3
4.4.1. Configuring Time Range	4-3
4.5. Monitoring and Maintaining Time Range	4-5
5. CONFIGURING HTTP	5-1
5.1. Overview	5-1
5.2. Features	5-1
5.2.1. Local HTTP Upgrade Service	5-3
5.3. Configuration	5-4
5.3.1. Configuring a Local HTTP Upgrade	5-4
6. CONFIGURING SYSLOG	6-1
6.1. Overview	6-1
6.2. Applications	6-1
6.2.1. Sending Syslogs to the Console	6-1
6.2.2. Sending Syslogs to the Log Server	6-2
6.3. Features	6-2
6.3.1. Logging	6-7
6.3.2. Syslog Format	6-8
6.3.3. Logging Direction	6-9
6.3.4. Syslog Filtering	6-11

6.3.5. Syslog Monitoring	6-13
6.4. Configuration	6-14
6.4.1. Configuring Syslog Format	6-16
6.4.2. Sending Syslogs to the Console	6-19
6.4.3. Sending Syslogs to the Monitor Terminal	6-22
6.4.4. Writing Syslogs into the Memory Buffer	6-24
6.4.5. Sending Syslogs to the Log Server	6-26
6.4.6. Writing Syslogs into Log Files	6-29
6.4.7. Configuring Syslog Filtering	6-32
6.4.8. Configuring Syslog Redirection	6-35
6.4.9. Configuring Syslog Monitoring	6-37
6.4.10. Synchronizing User Input with Log Output	6-39
6.5. Monitoring	6-40
7. CONFIGURING CWMP	7-1
7.1. Overview	7-1
7.2. Applications	7-1
7.2.1. CWMP Network Application Scenario	7-2
7.3. Features	7-2
7.3.1. Upgrading the Firmware	7-6
7.3.2. Upgrading the Configuration Files	7-7
7.3.3. Uploading the Configuration Files	7-8
7.3.4. Backing Up and Restoring a CPE	7-9
7.4. Configuration	7-9
7.4.1. Establishing a Basic CWMP Connection	7-10
7.4.2. Configuring CWMP-Related Attributes	7-15
7.5. Monitoring	7-21
8. CONFIGURING CA-MONITOR	8-1
8.1. Overview	8-1
8.2. Applications	8-1
8.2.1. Power-On/Power-Off	8-1
8.2.2. Intelligent Speed Adjustment of Fan	8-2
8.2.3. Intelligent Temperature Monitoring	8-3
8.3. Features	8-4
8.3.1. Automatic Power-Off of Line Cards	8-6
8.3.2. Manual Power-On/Power-Off of Line Cards	8-6
8.3.3. Intelligent Speed Adjustment of Fans	8-7
8.3.4. Intelligent Temperature Monitoring	8-7

8.4. Configuration	8-8
8.4.1. Configuring Power-On/Power-Off of Line Cards	8-9
8.4.2. Configuring the Operating Mode of Fans	8-10
8.4.3. Configuring Temperature Thresholds	8-12
8.5. Monitoring	8-13
9. CONFIGURING SOFTWARE AUTHORIZATION MANAGEMENT	9-1
9.1. Overview	9-1
9.2. Typical Application	9-1
9.2.1. VSD	9-1
9.2.1. FCoE	9-1
9.3. Function Details	9-2
9.3.1. Obtaining and Using a License File	9-3
9.3.2. Backing Up, Updating, and Removing a License File	9-5
9.4. Configuration Details	9-5
9.4.1. Basic Functions of Software Authorization	9-6
9.4.2. Backing Up License File	9-9
9.4.3. Friendly Period Warning	9-12
9.4.4. Updating License File	9-14
9.4.5. Removing License File	9-16
9.4.6. Unbinding License	9-18
9.5. Monitoring and Maintenance	9-20
10. CONFIGURING MODULE HOT SWAPPING	10-1
10.1. Overview	10-1
10.2. Applications	10-1
10.2.1. Resetting Online Modules	10-1
10.2.2. Clearing the Configuration of a Module	10-1
10.2.3. Clearing the Configuration of a VSU Member Device	10-2
10.2.4. Deleting the MAC Address from the Configuration File	10-2
10.2.5. Modifying a MAC Address in the Configuration File	10-3
10.3. Features	10-3
10.3.1. Automatically Installing the Inserted Module	10-3
10.3.2. Resetting Online Modules	10-4
10.4. Configuration	10-4
10.4.1. Clearing Module and Device Configuration	10-4
10.5. Monitoring	10-8
11. CONFIGURING SUPERVISOR MODULE REDUNDANCY	11-1
11.1. Overview	11-1

11.2. Applications	11-1
11.2.1. Redundancy of Supervisor Modules	11-2
11.3. Features	11-3
11.3.1. Election of Master and Slave Supervisor Modules	11-4
11.3.2. Information Synchronization of Supervisor Modules	11-6
11.4. Configuration	11-6
11.4.1. Configuring Manual Master/Slave Switching	11-7
11.4.2. Configuring the Automatic Synchronization Interval	11-9
11.4.3. Resetting Supervisor Modules	11-10
11.5. Monitoring	11-11
12. CONFIGURING USB	12-1
12.1. Overview	12-1
12.2. Applications	12-1
12.2.1. Using a USB Flash Drive to Upgrade a Device	12-1
12.3. Features	12-1
12.4. Configuration	12-2
12.4.1. Using a USB	12-2
12.4.2. Removing a USB	12-5
12.5. Monitoring	12-7
13. CONFIGURING POE	13-1
13.1. Overview	13-1
13.2. Applications	13-1
13.2.1. PoE Power Supply Scenario	13-1
13.3. Features	13-2
13.3.1. Power Supply Management for PoE Line Cards	13-3
13.3.2. Power Supply Management for the PoE System	13-4
13.3.3. Power Supply Management for PoE Ports	13-6
13.3.4. Auxiliary PoE Power Supply Functions	13-7
13.3.5. LLDP Classification	13-8
13.4. Configuration	13-9
13.4.1. Configuring PoE Power Supply on Line Cards	13-10
13.4.2. Configuring Power Supply of the PoE System	13-14
13.4.3. Configuring Power Supply on PoE Ports	13-17
13.4.4. Configuring Auxiliary PoE Power Supply Functions	13-22
13.4.5. Enabling the LLDP Classification	13-24
13.5. Monitoring	13-26

14. CONFIGURING UFT	14-1
14.1. Overview	14-1
14.2. Applications	14-1
14.2.1. Dynamic Entry Allocation	14-1
14.3. Features	14-2
14.3.1. UFT Operating Mode	14-2
14.4. Configuration	14-3
14.4.1. Configuring UFT Operating Mode	14-3
14.5. Monitoring	14-7
15. CONFIGURING PKG_MGMT	15-1
15.1. Overview	15-1
15.2. Applications	15-1
15.2.1. Upgrading/Degrading Subsystem	15-1
15.2.2. Upgrading Subsystem by One-click	15-2
15.2.3. Upgrading/Degrading a Single Feature Package	15-2
15.2.4. Installing a Hot Patch Package	15-2
15.2.5. Auto-Sync for Upgrade	15-3
15.3. Features	15-3
15.3.1. Upgrading/Degrading and Managing Subsystem Components	15-4
15.3.2. Upgrading/Degrading and Managing Functional Components	15-5
15.3.3. Upgrading/Degrading and Managing Hot Patch Packages	15-5
15.3.4. Auto-Sync for Upgrade	15-6
15.4. Configuration	15-7
15.4.1. Upgrading/Degrading a Firmware	15-8
15.4.2. Deactivating and Uninstalling a Hot Patch	15-22
15.4.3. Auto-Sync for Upgrade	15-24
15.5. Monitoring	15-26
16. CONFIGURING OPENFLOW	1
16.1. Overview	1
16.2. Typical Application	1
16.2.1. Centralized Control	1
16.3. Function Details	2
16.3.1. Separating Control from Forwarding	3
16.3.2. STP Control	4
16.4. Configuration Details	5
16.4.1. Configuring OpenFlow	5
16.5. Monitoring and Maintaining	11

1. CONFIGURING CLI

1.1. Overview

The command line interface (CLI) is a window used for text command interaction between users and network devices. You can enter commands in the CLI window to configure and manage network devices.

Protocols and Standards

N/A

1.2. Applications

Application	Description
Configuring and Managing Network Devices Through CLI	You can enter commands in the CLI window to configure and manage network devices

1.2.1. Configuring and Managing Network Devices Through CLI

Scenario

As shown in Figure 1-1, a user accesses network device A using a PC, and enter commands in the CLI window to configure and manage the network device.

Figure 1-1

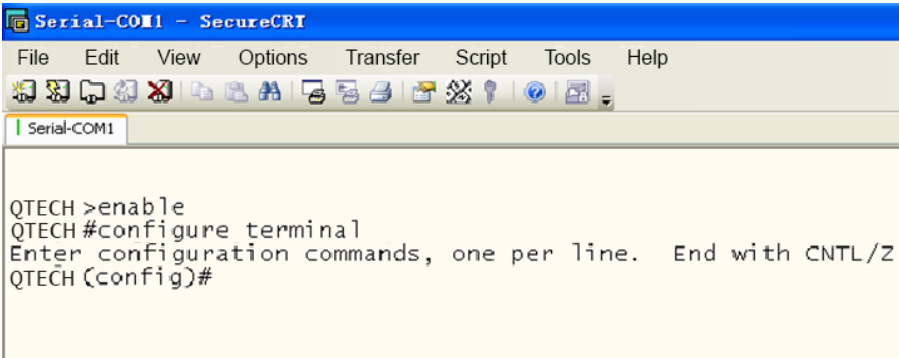


Remarks	A is the network device to be managed. PC is a terminal.
---------	---

Deployment

As shown in Figure 1-2, the user uses the Secure CRT installed on a PC to set up a connection with network device A, and opens the CLI window to enter configuration commands.

Figure 1-2



```

Serial-COM1 - SecureCRT
File Edit View Options Transfer Script Tools Help
Serial-COM1
QTECH >enable
QTECH #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
QTECH (config)#

```

1.3. Features

Overview

Feature	Description
Accessing CLI	You can log in to a network device for configuration and management.
Command Modes	The CLI provides several command modes. Commands that can be used vary according to command modes.
System Help.	You can obtain the help information of the system during CLI configuration.
Abbreviated Commands	If the entered string is sufficient to identify a unique command, you do not need to enter the full string of the command.
No and Default Options of Commands	You can use the no option of a command to disable a function or perform the operation opposite to the command, or use the default option of the command to restore default settings.
Prompts Indicating Incorrect Commands	An error prompt will be displayed if an incorrect command is entered.
History Commands	You can use short-cut keys to display or call history commands.
Featured Editing	The system provides short-cut keys for editing commands.
Searching and Filtering of the Show Command Output	You can run the show command to search or filter specified commands.
Command Alias	You can configure alias of a command to replace the command.

1.3.1. Accessing CLI

Before using the CLI, you need to connect a terminal or PC to a network device. You can use the CLI after starting the network device and finishing hardware and software initialization. When used for the first time, the network device can be connected only through the console

port, which is called out band management. After performing relevant configuration, you can connect and manage the network device through Telnet.

1.3.2. Command Modes

Due to the large number of commands, these commands are classified by function to facilitate the use of commands. The CLI provides several commands modes, and all commands are registered in one or several command modes. You must first enter the command mode of a command before using this command. Different command modes are related with each other while distinguished from each other.

As soon as a new session is set up with the network device management interface, you enter User EXEC mode. In this mode, you can use only a small number of commands and the command functions are limited, such as the **show** commands. Execution results of commands in User EXEC mode are not saved.

To use more commands, you must first enter Privileged EXEC mode. Generally, you must enter a password to enter Privileged EXEC mode. In Privileged EXEC mode, you can use all commands registered in this command mode, and further enter global configuration mode.

Using commands of a certain configuration mode (such as global configuration mode and interface configuration mode) will affect configuration in use. If you save the configuration, these commands will be saved and executed next time the system is restarted. You must enter global configuration mode before entering another configuration mode, such as interface configuration mode.

The following table summarizes the command modes by assuming that the name of the network device is "QTECH".

Command Mode	Access Method	Prompt	Exit or Entering Another Mode	About
User EXEC (User EXEC mode)	Enter User EXEC mode by default when accessing a network device.	QTECH>	Run the exit command to exit User EXEC mode. Run the enable command to enter Privileged EXEC mode.	Use this command mode to conduct basic tests or display system information.
Privileged EXEC (Privileged EXEC mode)	In User EXEC mode, run the enable command to enter Privileged EXEC mode.	QTECH#	Run the disable command to return to User EXEC mode. Run the configure command to enter global configuration mode.	Use this command mode to check whether the configuration takes effect. This mode is password protected.

Command Mode	Access Method	Prompt	Exit or Entering Another Mode	About
Global configuration (Global configuration mode)	In Privileged EXEC mode, run the configure command to enter global configuration mode.	QTECH(config)#	Run the exit or end command, or press Ctrl+C to return to Privileged EXEC mode. Run the interface command to enter interface configuration mode. When using the interface command, you must specify the interface. Run the vlan vlan_id command to enter VLAN configuration mode.	Using commands in this mode will affect the global parameters of the network device.
Interface configuration (Interface configuration mode)	In global configuration mode, run the interface command to enter interface configuration mode.	QTECH(config-if)#	Run the end command, or press Ctrl+C to return to Privileged EXEC mode. Run the exit command to return to global configuration mode. When using the interface command, you must specify the interface.	Use this configuration mode to configure various interfaces of the network device.
Config-vlan (VLAN configuration mode)	In global configuration mode, run the vlan vlan_id command to enter VLAN configuration mode.	QTECH(config-vlan)#	Run the end command, or press Ctrl+C to return to the Privileged EXEC mode. Run the exit command to return to global configuration mode.	Use this configuration mode to configure VLAN parameters.

1.3.3. System Help.

When entering commands in the CLI window, you can obtain the help information using the following methods:

1. At the command prompt in any mode, enter a question mark (?) to list the commands supported by the current command mode and related command description.

For example

```
QTECH>?
Exec commands:
<1-99>      Session number to resume
```

```
disable      Turn off privileged commands
disconnect   Disconnect an existing network connection
enable       Turn on privileged commands
exit         Exit from the EXEC
help         Description of the interactive help system
lock         Lock the terminal
ping         Send echo messages
show         Show running system information
telnet       Open a telnet connection
traceroute   Trace route to destination
```

2. Enter a space and a question mark (?) after a keyword of a command to list the next keyword or variable associated with the keyword.

For example

```
QTECH(config)#interface ?
Aggregateport  Aggregate port interface
Dialer         Dialer interface
GigabitEthernet Gigabit Ethernet interface
Loopback       Loopback interface
Multilink      Multilink-group interface
Null           Null interface
Tunnel         Tunnel interface
Virtual-ppp    Virtual PPP interface
Virtual-template Virtual Template interface
Vlan           Vlan interface
range         Interface range command
```

- ↪ If the keyword is followed by a parameter value, the value range and description of this parameter are displayed as follows:

```
QTECH(config)#interface vlan ?
<1-4094> Vlan port number
```

3. Enter a question mark (?) after an incomplete string of a command keyword to list all command keywords starting with the string.

For example

```
QTECH#d?  
debug delete diagnostic dir disable disconnect
```

4. After an incomplete command keyword is entered, if the suffix of this keyword is unique, press the Tab key to display the complete keyword.

For example

```
QTECH# show conf<Tab>  
QTECH# show configuration
```

5. In any command mode, run the help command to obtain brief description about the help system.

For example

```
QTECH(config)#help  
Help may be requested at any point in a command by entering  
a question mark '?'. If nothing matches, the help list will  
be empty and you must backup until entering a '?' shows the  
available options.  
Two styles of help are provided:  
1. Full help is available when you are ready to enter a  
command argument (e.g. 'show ?') and describes each possible  
argument.  
2. Partial help is provided when an abbreviated argument is entered  
and you want to know what arguments match the input  
(e.g. 'show pr?'.)
```

1.3.4. Abbreviated Commands

If a command is long, you can enter a part of the command that is sufficient to identify the command keyword.

For example, to run the interface gigabitEthernet 0/1 command in GigabitEthernet 0/1 interface configuration mode, enter the abbreviated command as follows:

```
QTECH(config)#int g0/1
QTECH(config-if-GigabitEthernet 0/1)#
```

1.3.5. No and Default Options of Commands

Most commands have the **no** option. Generally, the **no** option is used to disable a feature or function, or perform the operation opposite to the command. For example, run the **no shutdown** command to perform the operation opposite to the **shutdown** command, that is, enabling the interface. The keyword without the **no** option is used to enable a disabled feature or a feature that is disabled by default.

Most configuration commands have the **default** option. The **default** option is used to restore default settings of the command. Default values of most commands are used to disable related functions. Therefore, the function of the **default** option is the same as that of the **no** option in most cases. For some commands, however, the default values are used to enable related functions. In this case, the function of the **default** option is opposite to that of the **no** option. At this time, the **default** option is used to enable the related function and set the variables to default values.

↪ For specific function of the **no** or **default** option of each command, see the command reference.

1.3.6. Prompts Indicating Incorrect Commands

When you enter an incorrect command, an error prompt is displayed.

The following table lists the common CLI error messages.

Error Message	Meaning	How to Obtain Help
% Ambiguous command: "show c"	The characters entered are insufficient for identifying a unique command.	Re-enter the command, and enter a question mark after the word that is ambiguous. All the possible keywords will be displayed.
% Incomplete command.	The mandatory keyword or variable is not entered in the command.	Re-enter the command, and enter a space and a question mark. All the possible keywords or variables will be displayed.
% Invalid input detected at '^' marker.	An incorrect command is entered. The sign (^) indicates the position of the word that causes the error.	At the current command mode prompt, enter a question mark. All the command keywords allowed in this command mode will be displayed.

1.3.7. History Commands

The system automatically saves commands that are entered recently. You can use short-cut keys to display or call history commands.

The methods are described in the following table.

Operation	Result
Ctrl+P or the UP key	Display the previous command in the history command list. Starting from the latest record, you can repeatedly perform this operation to query earlier records.
Ctrl+N or the DOWN key	After pressing Ctrl+N or the DOWN key, you can return to a command that is recently executed in the history command list. You can repeatedly perform this operation to query recently executed commands.

1.3.8. Featured Editing

When editing the command line, you can use the keys or short-cut keys listed in the following table:

Function	Key or Short-Cut Key	Description
Move the cursor on the editing line.	Left key or Ctrl+B	Move the cursor to the previous character.
	Right key or Ctrl+B	Move the cursor to the next character.
	Ctrl+A	Move the cursor to the head of the command line.
	Ctrl+E	Move the cursor to the end of the command line.
Delete an entered character.	Backspace key	Delete one character to the left of the cursor.
	Delete key	Delete one character to the right of the cursor.
Move the output by one line or one page.	Return key	When displaying contents, press the Return key to move the output one line upward and display the next line. This operation is performed when the output does not end yet.
	Space key	When displaying contents, press the Space key to page down and display the next page. This operation is performed when the output does not end yet.

When the editing cursor is close to the right boundary, the entire command line will move to the left by 20 characters, and the hidden front part is replaced by the dollar (\$) signs. You can use the related keys or short-cut keys to move the cursor to the characters in the front or return to the head of the command line.

For example, the whole access-list may exceed the screen width. When the cursor is close to the end of the command line for the first time, the entire command line moves to the left by 20 characters, and the hidden front part is replaced by the dollar signs (\$). Each time the cursor is close to the right boundary, the entire command line moves to the left by 20 characters.

```
access-list 199 permit ip host 192.168.180.220 host
$ost 192.168.180.220 host 202.101.99.12
```



```
$0.220 host 202.101.99.12 time-range tr
```

Press **Ctrl+A** to return to the head of the command line. At this time, the hidden tail part of the command line is replaced by the dollar signs (\$).

```
access-list 199 permit ip host 192.168.180.220 host 202.101.99.$
```

↪ The default screen width is 80 characters.

1.3.9. Searching and Filtering of the Show Command Output

To search specified contents from the output of the show command, run the following command:

Command	Description
show any-command begin regular-expression	Searches specified contents from the output of the show command. The first line containing the contents and all information that follows this line will be output.

↪ The **show** command can be executed in any mode.

↪ Searched contents are case sensitive.

To filter specified contents from the output of the show command, run the following commands:

Command	Description
show any-command exclude regular-expression	Filters the output of the show command. Except those containing the specified contents, all lines will be output.
show any-command include regular-expression	Filters the output of the show command. Only the lines containing the specified contents will be output.

To search or filter the output of the **show** command, you must enter a vertical line (|). After the vertical line, select the searching or filtering rules and contents (character or string). Searched and filtered contents are case sensitive.

```
QTECH#show running-config | include interface
```

```
interface GigabitEthernet 0/0
```

```
interface GigabitEthernet 0/1
```

```
interface GigabitEthernet 0/2
```

```
interface GigabitEthernet 0/3
```

```
interface GigabitEthernet 0/4
```

```
interface GigabitEthernet 0/5
```



```
interface GigabitEthernet 0/6
interface GigabitEthernet 0/7
interface Mgmt 0
```

1.3.10. Command Alias

You can configure any word as the alias of a command to simplify the command input.

Configuration Effect

1. Replace a command with a word.

For example, configure "mygateway" as the alias of the ip route 0.0.0.0 0.0.0.0 192.1.1.1 command. To run this command, you only need to enter "mygateway".

2. Replace the front part of a command with a word, and enter the later part.

For example, configure "ia" as the alias of the ip address command. To run this command, you need to enter "ia" and then the specified IP address and subnet mask.

Configuration Steps

→ Displaying Default Alias

In User EXEC or Privileged EXEC mode, default alias are available for some commands. You can run the show aliases command to display these default aliases.

```
QTECH(config)#show aliases
Exec mode alias:
  h          help
  p          ping
  s          show
  u          undebug
  un        undebug
```

⚠ These default aliases cannot be deleted.

→ Configuring a Command Alias

Command	alias mode command-alias original-command
Parameter Description	<i>mode</i> : indicates the command mode of the command represented by the alias. <i>command-alias</i> : indicates the command alias. <i>original-command</i> : indicates the command represented by the alias.
Command Mode	Global configuration mode

Usage Guide	In global configuration mode, run the alias ? command to list all command modes that can be configured with aliases.
-------------	---

→ Displaying Settings of Command Aliases

Run the **show aliases** command to display alias settings in the system.

Notes

- The command replaced by an alias must start from the first character of the command line.
- The command replaced by an alias must be complete.
- The entire alias must be entered when the alias is used; otherwise, the alias cannot be identified.

Configuration Example

→ Defining an Alias to Replace the Entire Command

Configuration Steps	In global configuration mode, configure the alias "ir" to represent the default route configuration command <code>ip route 0.0.0.0 0.0.0.0 192.168.1.1</code> .
	<pre>QTECH#configure terminal QTECH(config)#alias config ir ip route 0.0.0.0 0.0.0.0 192.168.1.1</pre>
Verification	<ul style="list-style-type: none"> • Run the <code>show alias</code> command to check whether the alias is configured successfully. <pre>QTECH(config)#show alias Exec mode alias: h help p ping s show u undebug un undebug Global configuration mode alias: ir ip route 0.0.0.0 0.0.0.0 192.168.1.1</pre>
	<ul style="list-style-type: none"> • Use the configured alias to run the command, and run the <code>show running-config</code> command to check whether the alias is configured successfully.
	<pre>QTECH(config)#ir QTECH(config)#show running-config Building configuration... !</pre>

```
alias config ir ip route 0.0.0.0 0.0.0.0 192.168.1.1 //Configuring an
alias
...
ip route 0.0.0.0 0.0.0.0 192.168.1.1 //Configuration result after the
alias "ir" is entered
!
```

→ Defining an Alias to Replace the Front Part of a Command

Configurati on Steps	In global configuration mode, configure the alias "ir" to represent the front part "ip route" of the default route configuration command.
	<pre>QTECH#configure terminal QTECH(config)#alias config ir ip route</pre>
Verification	<ul style="list-style-type: none"> ● Run the show alias command to check whether the alias is configured successfully. <pre>QTECH(config)#show alias Exec mode alias: h help p ping s show u undebug un undebug Global configuration mode alias: ir ip route</pre>
	<ul style="list-style-type: none"> ● Enter the alias "ir" and then the later part of the command "0.0.0.0 0.0.0.0 192.168.1.1". ● Run the show ap-config running command to check whether the configuration is successful.
	<pre>QTECH(config)#ir 0.0.0.0 0.0.0.0 192.168.1.1 QTECH(config)#show running Building configuration... ! alias config ir ip route //Configuring an alias !</pre>

```
ip route 0.0.0.0 0.0.0.0 192.168.1.1 //Configuration result after the
alias "ir" and the later part of the command are entered
!
```

System Help

1. The system provides help information for command alias. An asterisk (*) will be displayed in front of an alias. The format is as follows:

```
*command-alias=original-command
```

For example, in Privileged EXEC mode, the default command alias "s" represents the show keyword. If you enter "s?", the keywords starting by "s" and alias information are displayed.

```
QTECH#s?
```

```
*s=show show start-chat start-terminal-service
```

2. If the command represented by an alias contains more than one word, the command is displayed in a pair of quotation marks.

For example, in Privileged EXEC mode, configure the alias "sv" to replace the show version command. If you enter "s?", the keywords starting by "s" and alias information are displayed.

```
QTECH#s?
```

```
*s=show *sv="show version" show start-chat
```

```
start-terminal-service
```

3. You can use the alias to obtain help information about the command represented by the alias.

For example, configure the alias "ia" to represent the **ip address** command in interface configuration mode. If you enter "ia?" in interface configuration mode, the help information on "ip address?" is displayed, and the alias is replaced by the command.

```
QTECH(config-if)#ia ?
```

```
A.B.C.D IP address
```

```
dhcp IP Address via DHCP
```

```
QTECH(config-if)#ip address
```

⚠ If you enter a space in front of a command, the command represented by this alias will not be displayed.

2. CONFIGURING BASIC MANAGEMENT

2.1. Overview

This document is a getting started guide to network device management. It describes how to manage, monitor, and maintain network devices.

2.2. Applications

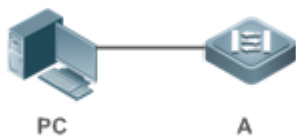
Application	Description
Network Device Management	A user logs in to a network device from a terminal and runs commands on a command line interface (CLI) to manage device configurations.

2.2.1. Network Device Management

Scenario

Network device management described in this document is performed through the CLI. A user logs in to Network Device A from a terminal and runs commands on the CLI to manage device configurations. See Figure 2-1.

Figure 2-1



2.3. Features

Basic Concepts

→ TFTP

Trivial File Transfer Protocol (TFTP) is a TCP/IP protocol which allows a client to transfer a file to a server or get a file from a server.

→ AAA

AAA is short for Authentication, Authorization and Accounting.

Authentication refers to the verification of user identities and the related network services.

Authorization refers to the granting of network services to users according to authentication results.

Accounting refers to the tracking of network service consumption by users. A billing system charges users based on consumption records.

AAA provides effective means of network management and security protection.

→ RADIUS

Remote Authentication Dial In User Service (RADIUS) is the most widely used AAA protocol at present.

→ Telnet

Telnet is a terminal emulation protocol in the TCP/IP protocol stack which provides access to a remote host through a virtual terminal connection. It is a standard protocol located at Layer 7 (application layer) of the Open System Interconnection (OSI) model and used on the internet for remote login. Telnet sets up a connection between the local PC and a remote host.

→ System Information

System information includes the system description, power-on time, hardware and software versions, control-layer software version, and boot-layer software version.

→ Hardware Information

Hardware information includes the physical device information as well as slot and module information. The device information includes the device description and slot quantity. The slot information includes the slot ID, module description (which is empty if a slot does not have a module), and actual and maximum number of physical ports.

Overview

Feature	Description
<u>User Access Control</u>	Controls the terminal access to network devices on the internet based on passwords and privileges.
<u>Login Authentication Control</u>	Performs username-password authentication to grant access to network devices when AAA is enabled. (Authentication is performed by a dedicated server.)
<u>Basic System Parameters</u>	Refer to the parameters of a system, such as the clock, banner, and Console baud rate.
<u>Displaying Configurations</u>	Displays the system configurations, including the configurations that the system is currently running and the device configurations stored in the nonvolatile random access memory (NVRAM).
<u>Configuration Rollback</u>	Allows you to configure the current configurations as a checkpoint and apply the checkpoint configurations to the device without restart.

Feature	Description
Telnet	Telnet is an application-layer protocol in the TCP/IP protocol stack. It provides the standard governing remote login and virtual terminal communication on the internet.
Restart	Introduces system restart.

2.3.1. User Access Control

User access control refers to the control of terminal access to network devices on the internet based on passwords and privileges.

Working Principle

→ Privilege Level

16 privilege levels are defined ranging from 0 to 15 for CLI on network devices to grant users access to different commands. Level 0 is the lowest level granting access to just a few commands, whereas level 15 is the highest level granting access to all commands. Levels 0 and 1 are common user levels without the device configuration permission (users are not allowed to enter global configuration mode by default). Levels 2–15 are privileged user levels with the device configuration permission.

→ Password Classification

Passwords are classified into two types: password and security. The first type refers to simple encrypted passwords at level 15. The second type refers to secure encrypted passwords at levels 0–15. If a level is configured with both simple and secure encrypted passwords, the simple encrypted password will not take effect. If you configure a non-15 level simple encrypted password, a warning is displayed and the password is automatically converted into a secure encrypted password. If you configure the same simple encrypted password and secure encrypted password at level 15, a warning is displayed.

→ Password Protection

Each privilege level on a network device has a password. An increase in privilege level requires the input of the target level password, whereas a reduction in privilege level does not require password input.

By default, only two privilege levels are password-protected, namely, level 1 (common user level) and level 15 (privileged user level). Sixteen privilege levels with password protection can be assigned to the commands in each mode to grant access to different commands.

If no password is configured for a privileged user level, access to this level does not require password input. It is recommended that a password be configured for security purposes.

→ Command Authorization

Each command has its lowest execution level. A user with a privilege level lower than this level is not allowed to run the command. After the command is assigned a privilege level, users at this level and higher have access to the command.

Related Configuration

→ Configuring a Simple Encrypted Password

- Run the **enable password** command.

→ Configuring a Secure Encrypted Password

- Run the **enable secret** command.
- A secure encrypted password is used to control the switching between user levels. It has the same function as a simple encrypted password but uses an enhanced password encryption algorithm. Therefore, secure encrypted passwords are recommended out of security consideration.

→ Configuring Command Privilege Levels

- Run the **privilege** command to assign a privilege level to a command.
- A command at a lower level is accessible by more users than a command at a higher level.
- To enable level increase logging, run the **login privilege log** command.

→ Raising/Lowering a User Privilege Level

- Run the **enable** command or the **disable** command to raise or lower a user privilege level respectively.
- After logging in to a network device, the user can change his/her level to obtain access to commands at different privilege levels.

→ Enabling Line Password Protection

- Line password protection is required for remote login (such as login through Telnet).
- Run the **password [0 | 7] line** command to configure a line password, and then run the **login** command to enable password protection.
- By default, terminals do not support the lock command.

2.3.2. Login Authentication Control

In login authentication with AAA disabled, the password entered by a user is checked against the configured line password. If they are consistent, the user can access the network device. In local authentication, the username and password entered by a user are checked against those stored in the local user database. If they are matched, the user can access the network device with proper management permissions.

In AAA, the username and password entered by a user are authenticated by a server. If authentication is successful, the user can access the network device and enjoy certain management permissions.

For example, a RADIUS server can be used to authenticate usernames and passwords and control users' management permissions on network devices. Network devices no longer store users' passwords, but send encrypted user information to the RADIUS server, including usernames, passwords, shared passwords, and access policies. This provides a convenient way to manage and control user access and improve user information security.

Working Principle

→ Line Password

If AAA is disabled, you can configure a line password used to verify user identities during login. After AAA is enabled, line password verification does not take effect.

→ Local Authentication

If AAA is disabled, you can configure local authentication to verify user identities and control management permissions by using the local user database. After AAA is enabled, local authentication does not take effect.

→ AAA

AAA provides three independent security functions, namely, Authentication, Authorization and Accounting. A server (or the local user database) is used to perform authentication based on the configured login authentication method list and control users' management permissions. For details about AAA, see Configuring AAA.

Related Configuration

→ Configuring Local User Information

- Run the **username** command to configure the account used for local identity authentication and authorization, including usernames, passwords, and optional authorization information.

→ Configuring Local Authentication for Line-Based Login

- Run the **login local** command (in the case that AAA is disabled).
- Perform this configuration on every device.

→ Configuring AAA Authentication for Line-Based Login

- The default authentication method is used after AAA is enabled.
- Run the **login authentication** command to configure a login authentication method list for a line.
- Perform this configuration when the local AAA authentication is required.

→ Configuring the Connection Timeout Time

- The default connection timeout time is 10 minutes.
- Run the **exec-timeout** command to change the default connection timeout time. An established connection will be closed if no output is detected during the timeout time.
- Perform this configuration when you need to increase or reduce the connection timeout time.

→ Configuring the Session Timeout Time

- The default session timeout time is 0 minutes, indicating no timeout.
- Run the **session-timeout** command to change the default session timeout time.
- The session established to a remote host through a line will be disconnected if no output is detected during the timeout time. Then the remote host is restored to Idle. Perform this configuration when you need to increase or reduce the session timeout time.

→ Locking a Session

- By default, terminals do not support the lock command.
- Run the lockable command to lock the terminals connected to the current line.
- To lock a session, first enable terminal lock in line configuration mode, and then run the lock command in terminal EXEC mode to lock the terminal.

2.3.3. Basic System Parameters

→ System Time

The network device system clock records the time of events on the device. For example, the time shown in system logs is obtained from the system clock. Time is recorded in the format of year-month-day, hour:minute:second, day of the week.

When you use a network device for the first time, set its system clock to the current date and time manually.

→ Configuring a System Name and Command Prompt

You can configure a system name to identify a network device. The default system name is QTECH. A name with more than 32 characters will be truncated to keep only the first 32 characters. The command prompt keeps consistent with the system name.

→ Banner

A banner is used to display login prompt information. There are two types of banner: Daily notification and login banner.

- Daily notification is displayed on all terminals connected to network devices soon after login. Urgent messages (such as immediate system shutdown) can be delivered to users through daily notification.

- A login banner appears after daily notification to display login information.

→ Configuring the Console Baud Rate

You can manage network device through a Console port. The first configuration on the network device must be performed through the Console port. The serial port baud rate can be changed based on actual requirements. Note that the management terminal must have consistent baud rate setting with the device console.

→ Configuring the Connection Timeout Time

The connection timeout time is used to control device connections (including established connections and sessions established to remote hosts). A connection will be closed when no input is detected during the timeout time.

Related Configuration

→ Configuring the System Date and Clock

- Run the **clock set** command to configure the system time of a network device manually. The device clock starts from the configured time and keeps running even when the device is powered off.

→ Updating the Hardware Clock

- If the hardware clock and software clock are not synchronized, run the **clock update-calendar** command to copy the date and time of the software clock to the hardware clock.

→ Configuring a System Name

- Run the **hostname** command to change the default system name.
- The default host name is **QTECH**.

→ Configuring a Command Prompt

- Run the prompt command.

→ Configuring Daily Notification

- By default, no daily notification is configured.
- Run the **banner motd** command to configure daily notification.
- Daily notification is displayed on all terminals connected to network devices soon after login. Urgent messages (such as immediate system shutdown) can be delivered to users through daily notification.

→ Configuring a Login Banner

- By default, no login banner is configured.
- Run the **banner login** command to configure a login banner to display login information.

→ Configuring the Console Baud Rate

- Run the **speed** command.

- The default baud rate is 9,600 bps.

2.3.4. Displaying Configurations

Displays the system configurations, including the configurations that the system is currently running and the device configurations stored in the NVRAM.

Working Principle

→ Running Configurations

Running configurations, namely, running-config, are the configurations that individual component modules run in real time. A request can be made to all running components to collect configurations, which will be orchestrated before being displayed to users. Only running components may provide real-time configurations, whereas unloaded components do not display configurations. In the case that the system is started, a component process is restarted, and a hot patch is executed, the configurations collected during this period may be inaccurate due to the component unstable state. For example, the configurations of a component may not be missing initially but can be displayed later.

→ Startup Configurations

The configurations stored in the NVRAM, namely, startup-config, are the configurations executed during device startup. When the system is restarted, startup-config is loaded to become new running-config. To display permanent configurations, the system needs to read the startup-config file in the NVRAM.

Related Configuration

→ Displaying Running Configurations

Run the **show running-config [interface *interface*]** command to display the configurations that the system is currently running or the configurations on an interface.

→ Displaying Startup Configurations

Run the **show startup-config** command.

→ Storing Startup Configurations

Run the **write** or **copy running-config startup-config** command to store the current running configurations as new startup configurations.

2.3.5. Configuration Rollback

Configuration rollback allows you to configure the current configurations as a snapshot or checkpoint and apply the checkpoint configurations to the device without restart.

Working Principle

An authorized user can create a checkpoint at any time as a copy of the current running configurations. The checkpoint is saved as a text file, which can be used to restore the running configurations at the checkpoint creation time. RGOS supports the creation of multiple checkpoints to store different versions of running configurations.

Related Configuration

→ Creating a Checkpoint

Run the **checkpoint** [*cp-name*] [**description** *description*] command to create a checkpoint. You can specify the checkpoint name and description.

→ Displaying Checkpoint Information

Run the **show checkpoint** { *cp-name* [**all**] | **summary** } command to display the information of a single or all checkpoints and the checkpoint summary.

→ Rolling Back Configurations

Run the **rollback running-config checkpoint** *cp-name* command to roll back the current configurations to a specific checkpoint configuration state.

→ Clearing Checkpoints

Run the **clear checkpoint database command** to delete all checkpoints and related configuration files.

2.3.6. Telnet

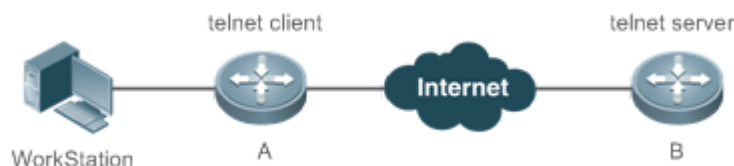
Working Principle

Telnet is an application-layer protocol in the TCP/IP protocol stack. It provides the standard governing remote login and virtual terminal communication on the internet.

The Telnet Client service allows a local or remote user who has logged in to a network device to use its Telnet Client program to access other remote system resources on the internet. In Figure 2-2, a user with a PC connects to Network Device A by using the terminal emulation or Telnet program and then logs in to Network Device B by using the telnet command to perform configuration management.

QTECH Telnet program supports the use of IPv4 and IPv6 addresses. A Telnet server accepts Telnet connection requests that carry IPv4 and IPv6 addresses. A Telnet client can send connection requests to hosts identified by IPv4 and IPv6 addresses.

Figure 2-2



Related Configuration

→ Enabling the Telnet Client Service

- Run the **telnet** command to log in to a remote device.

→ Restoring a Telnet Client Session

- Run the **<1-99>** command.

→ Disconnecting a Suspended Telnet Client Session

- Run the **disconnect** *session-id* command.

→ Enabling the Telnet Server Service

- Run the **enable service telnet-server** command.
- Perform this configuration when you need to enable Telnet login.

2.3.7. Restart

The timed restart feature makes user operation easier in some scenarios (such as tests).

- If you configure a time interval, the system will restart after the interval. The interval is in the format of *mmm* or *hhh:mm*, in the unit of minutes. You can specify the interval name to reflect the restart purpose.
- If you define a future time, the system will restart when the time is reached.

👉 The clock feature must be supported by the system if you want to use the **at** option. It is recommended that you configure the system clock in advance. A new restart plan will overwrite the existing one. A restart plan will be invalid if the system is restarted before the plan takes effect.

👉 The span between the restart time and current time must not exceed 31 days, and the restart time must be later than the current system time. After you configure a restart plan, do not to change the system clock; otherwise, the plan may fail (for example, the system time is changed to a time after the restart time.)

Related Configuration

→ Configuring Restart



- Run the **reload** command to configure a restart policy.
- Perform this configuration when you need to restart a device at a specific time.

Related Configuration

→ Batch-Running Commands

- Run **execute** to run the commands in batches.
- This command provides a convenient way to run multiple commands at a time.

2.4. Configuration

Configuring Passwords and Privileges	<p> (Optional) It is used to configure passwords and command privilege levels.</p>	
	enable password	Configures a simple encrypted password.
	enable secret	Configures a secure encrypted password.
	enable	Raises a user privilege level.
	login privilege log	Outputs log information of user privilege level increase.
	disable	Lowers a user privilege level.
	privilege	Configures command privilege levels.
	password	Specifies a line password.
	login	Enables line password protection.
Configuring Login and Authentication	<p> (Optional) It is used to configure different login modes and authentication methods.</p>	
	username	Configures local user account information and optional authorization information.
	login local	Configures local authentication for line-based login.
	login authentication	Configures AAA authentication for line-based login.
	telnet	Enables the Telnet Client service.
	enable service telnet-server	Enables the Telnet Server service.
	exec-timeout	Configures the connection timeout time.
	session-timeout	Configures the session timeout time.
lockable	Enables line-based terminal lock.	

	lock	Locks a terminal connected to the current line.
Configuring Basic System Parameters	👉 (Optional) It is used to configure basic system parameters.	
	clock set	Configures the system date and clock.
	clock update-calendar	Updates the hardware clock.
	hostname	Configures a system name.
	prompt	Configures a command prompt.
	banner motd	Configures daily notification.
	bannerlogin	Configures a login banner.
	speed	Configures the Console baud rate.
Enabling and Disabling a Specific Service	👉 (Optional) It is used to enable and disable a specific service.	
	enable service	Enables a service.
Rolling Back System Configurations	👉 (Optional) It is used to roll back system configurations.	
	checkpoint [cp-name] [description description]	Creates a configuration checkpoint.
	rollback running-config checkpoint cp-name	Rolls back configurations.
	clear checkpoint database	Clears checkpoints.
Configuring a Restart Policy	👉 (Optional) It is used to configure a system restart policy.	
	reload	Restarts a device.

2.4.1. Configuring Passwords and Privileges

Configuration Effect

- Configure passwords to control users' access to network devices.
- Assign a privilege level to a command to grant the command access to only the users at or higher than the level.
- Lower the command privilege level to grant more users access to the command.
- Raise the command privilege level to limit the command access to a few users.

Notes

- You can use the password configuration command with the **level** option to configure a password for a specific privilege level. After you specify the level and the password, the password works for the users who need to access this level.
- By default, no password is configured for any level. The default level is 15.
- If you configure a simple encrypted password with a non-15 level, a warning is displayed and the password is automatically converted into a secure encrypted password.
- The system chooses the secure encrypted password over the simple encrypted password if both of them are configured.

Configuration Steps

→ Configuring a Simple Encrypted Password

- (Optional) Perform this configuration when you need to establish simple encrypted password verification when users switch between different privilege levels.
- Run the **enable password** command to configure a simple encrypted password.

→ Configuring a Secure Encrypted Password

- (Optional) Perform this configuration when you need to establish secure encrypted password verification when users switch between different privilege levels.
- Run the **enable secret** command to configure a secure encrypted password.
- A secure encrypted password has the same function as a simple encrypted password but uses an enhanced password encryption algorithm. Therefore, secure encrypted passwords are recommended out of security consideration.

→ Configuring Command Privilege Levels

- Optional.
- A command at a lower level is accessible by more users than a command at a higher level.

→ Raising/Lowering a User Privilege Level

- After logging in to a network device, the user can change his/her level to obtain access to commands at different privilege levels.
- Run the **enable** command or the **disable** command to raise or lower a user privilege level respectively.
- To enable level increase logging, run the **login privilege log** command.

→ Enabling Line Password Protection

- (Optional) Line password protection is required for remote login (such as login through Telnet).
- Run the **password [0 | 7] line** command to configure a line password, and then run the **login** command to enable login authentication.

👉 If a line password is configured but login authentication is not configured, the system does not display password prompt.

Verification

- Run the **show privilege** command to display the current user level.
- Run the **show running-config** command to display the configuration.

Related Commands

→ Configuring a Simple Encrypted Password

Command	enable password [level level] { password [0 7] encrypted-password }
Parameter Description	<i>level</i> : Indicates a specific user level. <i>password</i> : Indicates the password used to enter privileged EXEC mode. <i>0</i> : Indicates that the password is entered in plaintext. <i>7</i> : Indicates that the password is entered in cyphertext. <i>encrypted-password</i> : Indicates the password text, which must contain case-sensitive English letters and digits. Leading spaces are allowed, but will be ignored. However, intermediate and trailing spaces are recognized.
Command Mode	Global configuration mode
Usage Guide	Currently, simple encrypted passwords can be configured with only level 15 and take effect only when no secure encrypted password is configured. If you configure a simple encrypted password with a non-15 level, a warning is displayed and the password is automatically converted into a secure encrypted password. If the level 15 simple encrypted password and secure encrypted password are configured the same, a warning is displayed. 👉 If you specify an encryption type and enter a password in plaintext, you cannot re-enter privileged EXEC mode. An encrypted password cannot be retrieved once lost. You have to configure a new password.


→ Configuring a Secure Encrypted Password

Command	enable secret [level level] { secret [0 5] encrypted-secret }
Parameter Description	<i>level</i> : Indicates a specific user level. <i>secret</i> : Indicates the password used to enter privileged EXEC mode. 0 5 : Indicates the password encryption type. 0 indicates no encryption, and 5 indicates secure encryption. <i>encrypted-password</i> : Indicates the password text.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure passwords for different privilege levels.

→ Raising a User Privilege Level

Command	enable [privilege-level]
Parameter Description	<i>privilege-level</i> : Indicates a specific privilege level.
Command Mode	Privileged EXEC mode
Usage Guide	An increase in privilege level requires the input of the target level password.

→ Lowering a User Privilege Level

Command	disable [privilege-level]
Parameter Description	<i>privilege-level</i> : Indicates a specific privilege level.
Command Mode	Privileged EXEC mode
Usage Guide	A reduction in privilege level does not require password input. Use this command to exit Privileged EXEC mode and return to user EXEC mode. If <i>privilege-level</i> is specified, the current privilege level is reduced to the specified level.  <i>privilege-level</i> must be lower than the current level.

→ Enabling Level Increase Logging

Command	login privilege log
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to enable logging of privilege level increase. The configuration takes effect for all terminals.

→ Configuring Command Privilege Levels

Command	privilege mode [all] { level level reset } <i>command-string</i>
Parameter Description	<i>mode</i> : Indicates the CLI mode of the command. For example, config indicates the global configuration mode, EXEC indicates the privileged command mode, and interface indicates the interface configuration mode. all : Changes the subcommand privilege levels of a specific command to the same level. level level : Indicates a privilege level, ranging from 0 to 15. reset : Restores the command privilege level to the default. <i>command-string</i> : Indicates the command to be assigned a privilege level.
Command Mode	Global configuration mode
Usage Guide	To restore a command privilege level, run the no privilege mode [all] level level <i>command</i> command in global configuration mode.

→ Specifying a Line Password

Command	<code>password [0 7] line</code>
Parameter Description	0: Indicates to configure a password in plaintext. 7: Indicates to configure a password in cyphertext. line: Indicates the password string.
Command Mode	Line configuration mode
Usage Guide	N/A

Enabling Line Password Protection

Command	<code>login</code>
Parameter Description	N/A
Command Mode	Line configuration mode
Usage Guide	N/A

Configuration Example

→ Configuring Command Authorization

Scenario	Assign privilege level 1 to the reload command and its subcommands and configure level 1 as the valid level (by configuring the test password).
Configuration Steps	<ul style="list-style-type: none"> Assign privilege level 1 to the reload command and its subcommands. <pre>QTECH# configure terminal QTECH(config)# privilege exec all level 1 reload QTECH(config)# enable secret level 1 0 test QTECH(config)# end</pre>
Verification	<ul style="list-style-type: none"> Check whether the reload command and its subcommands are accessible at level 1. <pre>QTECH# disable 1 QTECH> reload ? at reload at a specific time/date</pre>

```
cancel                cancel pending reload scheme
in                    reload after a time interval
<cr>
```

2.4.2. Configuring Login and Authentication

Configuration Effect

- Establish line-based login identity authentication.
- Run the **telnet** command on a network device to log in to a remote device.
- Close an established connection if no output is detected during the timeout time.
- Disconnect an established session connecting to a remote host and restore the host to Idle if no output is detected during the timeout time.
- Lock a terminal to deny access. When a user enters any character on the locked terminal, the password prompt is displayed. The terminal will be automatically unlocked if the entered password is correct.

Configuration Steps

→ Configuring Local User Information

- Mandatory.
- Run the **username** command to configure the account used for local identity authentication and authorization, including usernames, passwords, and optional authorization information.
- Perform this configuration on every device.

→ Configuring Local Authentication for Line-Based Login

- Mandatory.
- Configure local authentication for line-based login in the case that AAA is disabled.
- Perform this configuration on every device.

→ Configuring AAA Authentication for Line-Based Login

- (Optional) Perform this configuration to configure AAA authentication for line-based login.
- Configure AAA authentication for line-based login in the case that AAA is enabled.
- Perform this configuration on every device.

→ Enabling the Telnet Client Service

- Run the **telnet** command to log in to a remote device.

→ Restoring a Telnet Client Connection

- (Optional) Perform this configuration to restore the connection on a Telnet client.

→ Closing a Suspended Telnet Client Connection

- (Optional) Perform this configuration to close the suspended connection on a Telnet client.
- ➔ **Enabling the Telnet Server Service**
 - Optional.
 - Enable the Telnet Server service when you need to enable Telnet login.
- ➔ **Configuring the Connection Timeout Time**
 - Optional.
 - An established connection will be closed if no output is detected during the timeout time.
 - Perform this configuration when you need to increase or reduce the connection timeout time.
- ➔ **Configuring the Session Timeout Time**
 - Optional.
 - The session connecting to a remote host will be disconnected and the host be restored to Idle if no output is detected during the timeout time.
 - Perform this configuration when you need to increase or reduce the session timeout time.
- ➔ **Locking a Session**
 - (Optional) Perform this configuration when you need to temporarily exit a session on a device.
 - To lock a session, first enable terminal lock in line configuration mode, and then run the lock command to lock the terminal.

Verification

- Run the **show running-config** command to display the configuration.
- In the case that AAA is disabled, after local user information and line-based local authentication are configured, check whether users are prompted for username and password input for access to the CLI.
- In the case that AAA is enabled, after local user information and local AAA authentication are configured, check whether users are prompted for username and password input for access to the CLI.
- Run the **show user** command to display the information about the users who have logged in to the CLI.
- Telnet clients can connect to devices enabled with the Telnet Server service.
- When a user presses **Enter** on a locked CLI, the user is prompted for password input. The session is unlocked only when the entered password is the same as the configured one.
- Run the **show sessions** command to display every established Telnet client instance.

Related Commands

- ➔ **Configuring Local User Information**

Command	<code>username name [login mode { console ssh telnet }] [online amount number] [permission oper-mode path] [privilege privilege-level] [reject remote-login] [web-auth] [pwd-modify] [nopassword password [0 7] text-string]</code>
Parameter Description	<p>name: Indicates a user name.</p> <p>login mode: Indicates the login mode.</p> <p>console: Sets the login mode to Console.</p> <p>ssh: Sets the login mode to SSH.</p> <p>telnet: Sets the login mode to Telnet.</p> <p>online amount number: Indicates the maximum number of online accounts.</p> <p>permission oper-mode path: Configures the file operation permission. <code>op-mode</code> indicates the operation mode, and <code>path</code> indicates the directory or path of a specific file.</p> <p>privilege privilege-level: Indicates the account privilege level, ranging from 0 to 15.</p> <p>reject remote-login: Rejects remote login by using the account.</p> <p>web-auth: Allows only Web authentication for the account.</p> <p>pwd-modify: Allows the account owner to change the password. This option is available only when web-auth is configured.</p> <p>nopassword: Indicates that no password is configured for the account.</p> <p>password [0 7] text-string: Indicates the password configured for the account. 0 indicates that the password is input in plaintext, and 7 indicates that the password is input in cyphertext. The default is plaintext.</p>
Command Mode	Global configuration mode
Usage Guide	<p>Use this command to create a local user database to be used by authentication.</p> <p>If the value 7 is selected for the encryption type, the entered cyphertext string must consist of an even number of characters.</p> <p>This setting is applicable to the scenario where encrypted passwords may be copied and pasted. In other cases, the value 7 is not selected.</p>

→ Configuring Local Authentication for Line-Based Login

Command	<code>login local</code>
Parameter Description	N/A
Command Mode	Line configuration mode
Usage Guide	Use this command to configure local authentication for line-based login in the case that AAA is disabled. Local user information is configured by using the <code>username</code> command.

→ Configuring AAA Authentication for Line-Based Login

Command	<code>login authentication { default list-name }</code>
Parameter Description	<p>default: Indicates the default authentication method list name.</p> <p>list-name: Indicates the optional method list name.</p>
Command Mode	Line configuration mode

Usage Guide	Use this command to configure AAA authentication for line-based login in the case that AAA is enabled. The AAA authentication methods, including RADIUS authentication, local authentication, and no authentication, are used during the authentication process.
-------------	--

→ Enabling the Telnet Client Service

Command	telnet [oob] <i>host</i> [<i>port</i>] [/ source { ip A.B.C.D ipv6 X:X:X:X::X interface <i>interface-name</i> }] [/ vrf <i>vrf-name</i>] [via <i>mgmt-name</i>]
Parameter Description	oob : Remotely connects to a Telnet server through out-of-band communication (by using a management port). This option is available only when the device has a management port. host : Indicates the IPv4 address, IPv6 address, or host name of the Telnet server. port : Indicates the TCP port number of the Telnet server. The default value is 23. /source : Indicates the source IP address or source port used by a Telnet client. ip A.B.C.D: Indicates the source IPv4 address used by the Telnet client. ipv6 X:X:X:X::X: Indicates the source IPv6 address used by the Telnet client. interface <i>interface-name</i> : Indicates the source port used by the Telnet client. /vrf <i>vrf-name</i> : Indicates the name of the virtual routing and forwarding (VRF) table to be queried. via <i>mgmt-name</i> : Indicates the management port used by the Telnet client when the oob option is specified.
Command Mode	Privileged EXEC mode
Usage Guide	A user can telnet to a remote device identified by an IPv4 host name, IPv6 host name, IPv4 address, or IPv6 address.

→ Restoring a Telnet Client Session

Command	<1-99>
Parameter Description	N/A
Command Mode	User EXEC mode
Usage Guide	Use this command to restore a Telnet client session. A user can press the shortcut key Ctrl+Shift+6 X to temporarily exit the Telnet client session that is established using the telnet command, run the <1-99> command to restore the session, and run the show sessions command to display the session information.

→ Closing a Suspended Telnet Client Connection

Command	disconnect <i>session-id</i>
Parameter Description	<i>session-id</i> : Indicates the suspended Telnet client session ID.
Command Mode	User EXEC mode
Usage Guide	Use this command to close a specific Telnet client session by entering the session ID.

→ Enabling the Telnet Server Service

Command	enable service telnet-server
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to enable the Telnet Server service. The IPv4 and IPv6 services are also enabled after the command is executed.

→ Configuring the Connection Timeout Time

Command	exec-timeout <i>minutes</i> [<i>seconds</i>]
Parameter Description	<i>minutes</i> : Indicates the connection timeout time in the unit of minutes. <i>seconds</i> : Indicates the connection timeout time in the unit of seconds.
Command Mode	Line configuration mode
Usage Guide	Use this command to configure the timeout time for the established connections on a line. A connection will be closed when no input is detected during the timeout time. To remove the connection timeout configuration, run the no exec-timeout command in line configuration mode.

→ Configuring the Session Timeout Time

Command	session-timeout <i>minutes</i> [<i>output</i>]
Parameter Description	<i>minutes</i> : Indicates the session timeout time in the unit of minutes. output : Indicates whether to add data output as a timeout criterion.
Command Mode	Line configuration mode
Usage Guide	Use this command to configure the timeout time for the remote host sessions on a line. A session will be disconnected when no input is detected during the timeout time. To cancel the session timeout time, run the no session-timeout command in line configuration mode.

→ Enabling Line-Based Terminal Lock

Command	lockable
Parameter Description	N/A
Command Mode	Line configuration mode
Usage Guide	N/A

→ Locking a Terminal Connected to the Current Line

Command	lock
---------	------

Parameter Description	N/A
Command Mode	Line configuration mode
Usage Guide	N/A

Configuration Example

→ Establishing a Telnet Session to a Remote Network Device

Configuration Steps	<ul style="list-style-type: none"> Establish a Telnet session to a remote network device with the IP address 192.168.65.119. Establish a Telnet session to a remote network device with the IPv6 address 2AAA:BBBB::CCCC.
	<pre>QTECH# telnet 192.168.65.119 Trying 192.168.65.119 ... Open User Access Verification Password:</pre>
	<pre>QTECH# telnet 2AAA:BBBB::CCCC Trying 2AAA:BBBB::CCCC ... Open User Access Verification Password:</pre>
Verification	<ul style="list-style-type: none"> Check whether the Telnet sessions are established to the remote network devices.

→ Configuring the Connection Timeout Time

Configuration Steps	<ul style="list-style-type: none"> Set the connection timeout time to 20 minutes.
	<pre>QTECH# configure terminal //Enter global configuration mode. QTECH# line vty 0 //Enter line configuration mode. QTECH(config-line)#exec-timeout 20 //Set the connection timeout time to 20 minutes.</pre>
Verification	<ul style="list-style-type: none"> Check whether the connection between a terminal and the local device is closed when no input is detected during the timeout time.

→ Configuring the Session Timeout Time

Configuration Steps	<ul style="list-style-type: none"> ● Set the session timeout time to 20 minutes.
	<pre>QTECH# configure terminal //Enter global configuration mode. QTECH(config)# line vty 0 //Enter line configuration mode. QTECH(config-line)#session-timeout 20 //Set the session timeout time to 20 minutes.</pre>
Verification	Check whether the session between a terminal and the local device is disconnected when no input is detected during the timeout time.

2.4.3. Configuring Basic System Parameters

Configuration Effect

- Configure basic system parameters.

Configuration Steps

→ Configuring the System Date and Clock

- Mandatory.
- Configure the system time of a network device manually. The device clock starts from the configured time and keeps running even when the device is powered off.

👉 The time configuration is applied only to the software clock if the network device does not provide a hardware clock. The configuration will be invalid when the device is powered off.

→ Updating the Hardware Clock

- Optional.
- Perform this configuration when you need to copy the date and time of the software clock to the hardware clock so that the hardware clock is synchronized with the software clock.

→ Configuring a System Name

- (Optional) Perform this configuration to change the default system name.

→ Configuring a Command Prompt

- (Optional) Perform this configuration to change the default command prompt.

→ Configuring Daily Notification

- (Optional) Perform this configuration when you need to display important prompts or warnings to users.
- You can configure notification in one or multiple lines, which will be displayed to users after login.

→ Configuring a Login Banner

- (Optional) Perform this configuration when you need to display important messages to users upon login or logout.

→ Configuring the Console Baud Rate

- (Optional) Perform this configuration to change the default Console baud rate.

Verification

- Run the **show clock** command to display the system time.
- Check whether a login banner is displayed after login.
- Run the **show version** command to display the system information and version.

Related Commands

→ Configuring the System Date and Clock

Command	clock set hh:mm:ss month day year
Parameter Description	<i>hh:mm:ss</i> : Indicates the current time, in the format of hour (24-hour format): <i>minute:second</i> . <i>day</i> : Indicates a day (1–31) of the month. <i>month</i> : Indicates a month (from January to December) of the year. <i>year</i> : Indicates a year, ranging from 1993 to 2035. Abbreviation is not supported.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to configure the system time. If the device does not provide a hardware clock, the time configuration will be invalid when the device is powered off.

→ Updating the Hardware Clock

Command	clock update-calendar
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	After the configuration, the time of the software clock will overwrite that of the hardware clock.

→ Configuring a System Name

Command	hostname <i>name</i>
Parameter Description	<i>name</i> : Indicates the system name, which must consist of printable characters and must not exceed 63 bytes.
Command Mode	Global configuration mode
Usage Guide	To restore the system name to the default, run the no hostname command in global configuration mode.

→ Configuring a Command Prompt

Command	prompt <i>string</i>
---------	-----------------------------

Parameter Description	<i>string</i> : Indicates the command prompt name. A name with more than 32 characters will be truncated to keep only the first 32 characters.
Command Mode	Privileged EXEC mode
Usage Guide	To restore the command prompt to the default settings, run the no prompt command in global configuration mode.

→ Configuring Daily Notification

Command	banner motd c message c
Parameter Description	c: Indicates a delimiter, which can be any character, such as "&".
Command Mode	Global configuration mode
Usage Guide	A message must start and end with delimiter+carriage return respectively. Any characters following the ending delimiter will be dropped. Any letter contained in the message must not be used as the delimiter. The message must not exceed 255 bytes.

→ Configuring a Login Banner

Command	banner login c message c
Parameter Description	c: Indicates a delimiter, which can be any character, such as "&".
Command Mode	Global configuration mode
Usage Guide	A message must start and end with delimiter+carriage return respectively. Any characters following the ending delimiter will be dropped. Any letter contained in the message must not be used as the delimiter. The message must not exceed 255 bytes. To remove the login banner configuration, run the no banner login command in global configuration mode.

→ Configuring the Console Baud Rate

Command	speed speed
Parameter Description	<i>speed</i> : Indicates the console baud rate, in the unit of bps. The serial port baud rate can be set to 9,600 bps, 19,200 bps, 38,400 bps, 57,600 bps, or 115,200 bps. The default is 9,600 bps.
Command Mode	Line configuration mode
Usage Guide	You can configure the asynchronous line baud rate based on requirements. The speed command is used to configure receive and transmit rates for the asynchronous line.

Configuration Example

→ Configuring the System Time

Configuration Steps	<ul style="list-style-type: none"> Change the system time to 2003-6-20, 10:10:12.
	<pre>QTECH# clock set 10:10:12 6 20 2003 //Configure the system time and date.</pre>
Verification	<ul style="list-style-type: none"> Run the show clock command in privileged EXEC mode to display the system time.
	<pre>QTECH# show clock //Confirm that the changed system time takes effect. clock: 2003-6-20 10:10:54</pre>

→ Configuring Daily Notification

Configuration Steps	<ul style="list-style-type: none"> Configure the daily notification message "Notice: system will shutdown on July 6th." with the pound key (#) as the delimiter.
	<pre>QTECH(config)# banner motd #//Starting delimiter Enter TEXT message. End with the character '#'. Notice: system will shutdown on July 6th.# //Ending delimiter QTECH(config)#</pre>
Verification	<ul style="list-style-type: none"> Run the show running-config command to display the configuration. Connect to the local device through the Console, Telnet or SSH, and check whether daily notification is displayed before the CLI appears.
	<pre>C:\>telnet 192.168.65.236 Notice: system will shutdown on July 6th. Access for authorized users only. Please enter your password. User Access Verification Password:</pre>

→ Configuring a Login Banner

Configuration Steps	<ul style="list-style-type: none"> Configure the login banner message "Access for authorized users only. Please enter your password." with the pound key (#) as the delimiter.
	<pre>QTECH(config)# banner login #//Starting delimiter Enter TEXT message. End with the character '#'. Access for authorized users only. Please enter your password. # //Ending delimiter QTECH(config)#</pre>

Verification	<ul style="list-style-type: none"> ● Run the <code>show running-config</code> command to display the configuration. ● Connect to the local device through the Console, Telnet or SSH, and check whether the login banner is displayed before the CLI appears.
	<pre>C:\>telnet 192.168.65.236 Notice: system will shutdown on July 6th. Access for authorized users only. Please enter your password. User Access Verification Password:</pre>

→ Configuring the Serial Port Baud Rate

Configuration Steps	<ul style="list-style-type: none"> ● Set the serial port baud rate to 57,600 bps.
	<pre>QTECH# configure terminal //Enter global configuration mode. QTECH(config)# line console 0 //Enter console line configuration mode. QTECH(config-line)# speed 57600 //Set the console baud rate to 57,600 bps. QTECH(config-line)# end //Returns to privileged mode.</pre>
Verification	<ul style="list-style-type: none"> ● Run the show command to display the configuration.
	<pre>QTECH# show line console 0 //Displays the console configuration. CON Type speed Overruns * 0 CON 57600 0 Line 0, Location: "", Type: "vt100" Length: 25 lines, Width: 80 columns Special Chars: Escape Disconnect Activation ^^x none ^M Timeouts: Idle EXEC Idle Session never never History is enabled, history size is 10. Total input: 22 bytes Total output: 115 bytes Data overflow: 0 bytes stop rx interrupt: 0 times Modem: READY</pre>

2.4.4. Enabling and Disabling a Specific Service

Configuration Effect

- Dynamically adjust system services when the system is running, and enable and disable specific services (SNMP Agent, SSH Server, and Telnet Server).

Configuration Steps

→ Enabling the SNMP Agent, SSH Server, and Telnet Server Services

- (Optional) Perform this configuration when you need to use these services.

Verification

- Run the show running-config command to display the configuration.
- Run the show services command to display the service Enabled/Disable state.

Related Commands

→ Enabling the SSH Server, Telnet Server, and SNMP Agent Services

Command	enable service { ssh-server telnet-server snmp-agent }
Parameter Description	ssh-server: Enables or disables the SSH Server service. The IPv4 and IPv6 services are also enabled together with this service. telnet-server: Enables or disables the Telnet Server service. The IPv4 and IPv6 services are also enabled together with this service. snmp-agent: Enables or disables the SNMP Agent service. The IPv4 and IPv6 services are also enabled together with this service.
Command Mode	Global configuration mode
Usage Guide	Use this command to enable and disable specific services.

Configuration Example

→ Enabling the SSH Server Service

Configuration Steps	<ul style="list-style-type: none">• Enable the SSH Server service.
	<pre>QTECH# configure terminal //Enter global configuration mode. QTECH(config)#enable service ssh-server //Enable the SSH Server service.</pre>
Verification	<ul style="list-style-type: none">• Run the show running-config command to display the configuration.• Run the show ip ssh command to display the configuration and running state of the SSH Server service.

2.4.5. Rolling Back System Configurations

Configuration Effect

After a checkpoint is configured on a device, a copy of the device running configurations at the checkpoint creation time is saved. The copy can be used to restore the current system configurations to the state at the checkpoint creation time.

Notes

N/A

Configuration Steps

→ Creating a Checkpoint

- Optional.
- Run the **checkpoint** command in privileged EXEC mode to create a checkpoint, that is, a copy of the current running configurations.
- Run the **show checkpoint** command in privileged EXEC mode to display the checkpoint information.

→ Rolling Back Configurations

- (Optional) Perform this configuration when you need to roll back the device configurations to checkpoint configurations.
- Run the **rollback** command in privileged EXEC mode to apply the checkpoint configurations.

→ Clearing Checkpoints

- (Optional) Perform this configuration when you need to clear all checkpoints.
- Run the **clear checkpoint** database command in privileged EXEC mode to delete all checkpoints.

Verification

- Run the **show running-config** command to display the current running configurations.
- Run the **show checkpoint** command to display the checkpoint used for rollback. Run the **more** command to open the checkpoint configuration file and check the content.
- Run the **rollback** command to perform rollback. When rollback is completed, run the **show running-config** command and check whether the checkpoint configurations are applied.


Related Commands

→ Creating a Checkpoint

Command	checkpoint [<i>cp-name</i>] [description <i>description</i>]
Parameter Description	<i>cp-name</i> : Indicates the checkpoint name, which consists of one to 80 characters. description <i>description</i> : Indicates the checkpoint description, which contains up to 80 characters.
Defaults	N/A

Command Mode	Privileged EXEC mode
Usage Guide	Use this command to create a checkpoint and specify its name and description.

→ Rolling Back Configurations

Command	rollback running-config checkpoint <i>cp-name</i> [display-differences ignore-results]
Parameter Description	<i>cp-name</i> : Indicates the checkpoint name, which consists of one to 80 characters.
Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	 Use this command to roll back the current running configurations to a specific checkpoint.

→ Clearing Checkpoints

Command	clear checkpoint database
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to delete all checkpoints and related configuration files.

2.4.6. Configuring a Restart Policy

Configuration Effect

Configure a restart policy to restart a device as scheduled.

Configuration Steps

→ Configuring Direct Restart

Run the **reload** command in privileged EXEC mode to restart the system immediately.

→ Configuring Timed Restart

```
reload in mmm | hhh:mm [string]
```

If you configure a time interval, the system will restart after the interval. The interval is in the format of mmm or hhh:mm, in the unit of minutes. You can specify the interval name by using the string parameter to reflect the restart purpose.

```
reload at hh:mm month day year [string]
```

If you configure a specific time, the system will restart at the time. The time must be a time in the future. The year parameter is optional. If it is not specified, the year of the system clock is used by default. Because the span between the restart time and current time must not exceed 31 days, the year parameter does not need to be specified if the current system time falls between January 1 and November 30. If the current system time falls on December, the restart time may and can be a time on January next year. You need to specify the year to notify the system that the restart time is on January next year instead of January of the current year. If the year is not specified, the restart time is on January of the current year by default, causing a restart failure.

- 👉 The clock feature must be supported by the system if you want to use the `at` option. It is recommended that you configure the system clock in advance. A new restart plan will overwrite the existing one. A restart plan will be invalid if the system is restarted before the plan takes effect.
- 👉 The span between the restart time and current time must not exceed 31 days, and the restart time must be later than the current system time. After you configure a restart plan, do not change the system clock; otherwise, the plan may fail (for example, the system time is changed to a time after the restart time.)

→ Deleting a Restart Policy

Run the **reload cancel** command to delete a restart policy.

Related Commands

→ Restarting a Device

Command	reload [<i>text</i> <i>in</i> [<i>hh</i> :] <i>mm</i> [<i>text</i>] <i>at</i> <i>hh:mm</i> [<i>month day year</i>] [<i>text</i>] cancel]
Parameter Description	<i>text</i> : Indicates the restart reason, which consists of one to 255 bytes. <i>in</i> [<i>hh</i> :] <i>mm</i> : Indicates the time interval after which the system will restart. The maximum interval is 24 days. <i>at</i> <i>hh:mm</i> : Indicates the time when the system will restart. <i>month</i> : Indicates a month of the year. (For example, Mar indicates March.) <i>day</i> : Indicates a date, ranging from 1 to 31. <i>year</i> : Indicates a year, ranging from 1993 to 2035. Abbreviation is not supported. cancel : Cancels the restart plan.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to enable a device to restart at a specific time.

2.5. Monitoring

Displaying

Description	Command
-------------	---------

show checkpoint { <i>cp-name</i> [all] summary }	Displays checkpoint information or summary.
show clock	Displays the current system time.
show line { console <i>line-num</i> vty <i>line-num</i> <i>line-num</i> }	Displays line configurations.
show reload	Displays system restart settings.
show running-config [interface <i>interface</i>]	Displays the current running configurations of the device or the configurations on an interface.
show startup-config	Displays the device configurations stored in the NVRAM.
show this	Displays the current system configurations.
show version [devices module slots]	Displays system information.
show sessions	Displays the information of each established Telnet client instance.

3. CONFIGURING LINES

3.1. Overview

There are various types of terminal lines on network devices. You can manage terminal lines in groups based on their types. Configurations on these terminal lines are called line configurations. On network devices, terminal lines are classified into multiple types such as CTY, and VTY.

3.2. Applications

Application	Description
Accessing a Device Through Console	Enter the command-line interface (CLI) of a network device through the Console.
Accessing a Device Through VTY	Enter the CLI of a network device through Telnet or SSH.

3.3.1. Accessing a Device Through Console

Scenario

Figure 3-1



Remarks	A is a network device to be managed. PC is a network management station.
---------	---

Deployment

The network management station connects to the Console port of a network device through a serial cable. Using the Console software (Hyper Terminal or other terminal simulation software) on the network management station, you can access the Console of the network device and enter the CLI to configure and manage the network device.

3.3.1. Accessing a Device Through VTY

Scenario

Figure 3-2



Remarks	A is a network device to be managed. PC is a network management station.
---------	---

Deployment

The network management station connects to a network device through the network. Using a VTY client (such as Putty) on the network management station, you can access the network device through Telnet or SSH and enter the CLI to configure and manage the network device.

3.3. Features

Basic Concepts

→ CTY

The CTY line refers to the line connected to the Console port. Most network devices have a Console port. You can access the local system through the Console port.

→ VTY

The VTY line is a virtual terminal line that does not correspond to any hardware. It is used for Telnet or SSH connection.

Overview

Feature	Description
Basic Features	Configures a terminal, displays and clears terminal connection information.

3.3.1. Basic Features

Related Configuration

→ Configuring Terminal Lines

Run the line command in global configuration mode to enter the configuration mode of a specified line.

Configure the line attributes.

→ Clearing Terminal Connections

When a terminal connects to the network device, the corresponding terminal line is occupied. Run the **show user** command to display the connection status of these terminal lines. If you want to disconnect the terminal from the network device, run the **clear line** command to clear


the terminal line. After the terminal lines are cleared, the related connections (such as Telnet and SSH) are interrupted, the CLI exits, and the terminal lines restore to the unoccupied status. Users can re-establish connections.

→ Specifying the Number of VTY Terminals

Run the **line vty** command to enter the VTY line configuration mode and specify the number of VTY terminals.

By default, there are 5 VTY terminals, numbered from 0 to 4. You can increase the number of VTY terminals to 36, with new ones numbered from 5 to 35. Only new terminals can be removed.

3.4. Configuration

Configuration	Description and Command
	 (Mandatory) It is used to enter the line configuration mode.
line [console vty] first-line [last-line]	Enters the specified line configuration mode.
line vty line-number	Increases or reduces the number of available VTY lines.

3.4.1. Entering Line Configuration Mode

Configuration Effect

Enter line configuration mode to configure other functions.

Configuration Steps

→ Entering Line Configuration Mode

- Mandatory.
- Unless otherwise specified, enter line configuration mode on each device to configure line attributes.

→ Increasing/Reducing the Number of VTY Lines

- Optional.
- Run the **(no) line vty line-number** command to increase or reduce the number of VTY lines.

Verification

Run the **show line** command to display line configuration.

Related Commands

→ Entering Line Configuration Mode

Command	line [console vty] first-line [last-line]
Parameter Description	console: Indicates the Console port. vty: Indicates a virtual terminal line, which supports Telnet or SSH. <i>first-line:</i> Indicates the number of the first line. <i>last-line:</i> Indicates the number of the last line.
Command Mode	Global configuration mode
Usage Guide	N/A


→ Increasing/Reducing the Number of VTY Lines

Command	line vty line-number
Parameter Description	<i>line-number:</i> Indicates the number of VTY lines. The value ranges from 0 to 35.
Command Mode	Global configuration mode
Usage Guide	Run the no line vty line-number command to reduce the number of available VTY lines.

→ Displaying Line Configuration

Command	show line { console line-num vty line-num line-num }
Parameter Description	console: Indicates the Console port. vty: Indicates a virtual terminal line, which supports Telnet or SSH. <i>line-num:</i> Indicates the line to be displayed.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuration Example

Scenario Figure 3-3	 <p>The diagram illustrates a PC on the left connected to a network device labeled 'A' on the right. A line representing the console connection is shown between them.</p>
Configuration Steps	<ul style="list-style-type: none"> ● Connect the PC to network device A through the Console line and enter the CLI on the PC. ● Run the show user command to display the connection status of the terminal line.

	<ul style="list-style-type: none"> ● Run the <code>show line console 0</code> command to display the status of the Console line. ● Enter global configuration mode and run the <code>line vty</code> command to increase the number of VTY terminals to 36.
A	<pre> QTECH#show user Line User Host(s) Idle Location ----- * 0 con 0 --- idle 00:00:00 --- QTECH#show line console 0 CON Type speed Overruns * 0 CON 9600 0 Line 0, Location: "", Type: "vt100" Length: 24 lines, Width: 79 columns Special Chars: Escape Disconnect Activation ^^x ^D ^M Timeouts: Idle EXEC Idle Session 00:10:00 never History is enabled, history size is 10. Total input: 490 bytes Total output: 59366 bytes Data overflow: 0 bytes stop rx interrupt: 0 times QTECH#show line vty ? <0-5> Line number QTECH#configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)#line vty 35 QTECH(config-line)# *Oct 31 18:56:43: %SYS-5-CONFIG_I: Configured from console by console </pre>
Verification	<ul style="list-style-type: none"> ● After running the <code>show line</code> command, you can find that the number of terminals increases.

- Run the show running-config command to display the configuration.

A

```
QTECH#show line vty ?
  <0-35>  Line number

QTECH#show running-config

Building configuration...
Current configuration : 761 bytes

version 11.0(1C2B1) (10/16/13 04:23:54 CST -ngcf78)
ip tcp not-send-rst
vlan 1
!
interface GigabitEthernet 0/0
!
interface GigabitEthernet 0/1
  ip address 192.168.23.164 255.255.255.0
!
interface GigabitEthernet 0/2
!
interface GigabitEthernet 0/3
!
interface GigabitEthernet 0/4
!
interface GigabitEthernet 0/5
!
interface GigabitEthernet 0/6
!
interface GigabitEthernet 0/7
!
interface Mgmt 0
!
line con 0
line vty 0 35
  login
!
```

```
end
```

3.5. Monitoring

Clearing

⚠ Running the clear commands may lose vital information and thus interrupt services.

Description	Command
Clears the line connection status.	clear line { console line-num vty line-num line-num }

Displaying

Description	Command
Displays the line configuration.	show line { console line-num vty line-num line-num }

4. CONFIGURING TIME RANGE

4.1. Overview

Time Range is a time-based control service that provides some applications with time control. For example, you can configure a time range and associate it with an access control list (ACL) so that the ACL takes effect within certain time periods of a week.

4.2. Typical Application

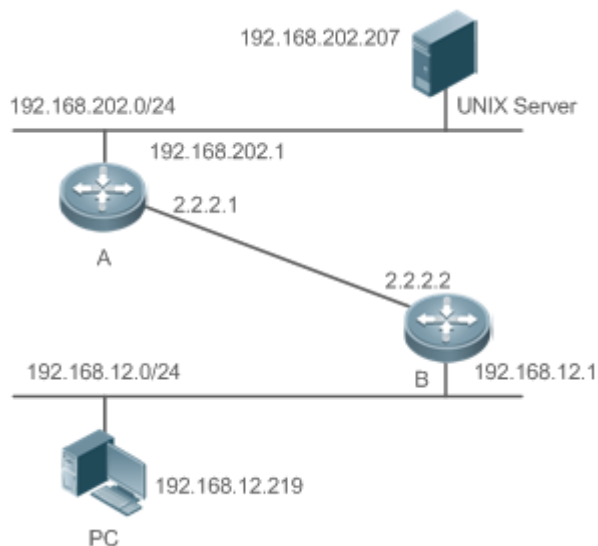
Typical Application	Scenario
Applying Time Range to an ACL	Apply a time range to an ACL module so that the time-based ACL takes effect

4.2.1. Applying Time Range to an ACL

Application Scenario

An organization allows users to access the Telnet service on a remote Unix host during working hours only, as shown in Figure 4-1.

Figure 4-1



Note	Configure an ACL on device B to implement the following security function: Hosts in network segment 192.168.12.0/24 can access the Telnet service on a remote Unix host during normal working hours only.
------	--

Functional Deployment

- On device B, apply an ACL to control Telnet service access of users in network segment 192.168.12.0/24. Associate the ACL with a time range, so that the users' access to the Unix host is allowed only during working hours.

4.3. Function Details

Basic Concepts

→ Absolute Time Range

The absolute time range is a time period between a start time and an end time. For example, [12:00 January 1 2000, 12:00 January 1 2001] is a typical absolute time range. When an application based on a time range is associated with the time range, a certain function can be effective within this time range.

→ Periodic Time

Periodic time refers to a periodical interval in the time range. For example, “from 8:00 every Monday to 17:00 every Friday” is a typical periodic time interval. When a time-based application is associated with the time range, a certain function can be effective periodically from every Monday to Friday.

Features

Feature	Function
<u>Using Absolute Time Range</u>	Sets an absolute time range for a time-based application, so that a certain function takes effect within the absolute time range.
<u>Using Periodic Time</u>	Sets periodic time or a time-based application, so that a certain function takes effect within the periodic time.

4.3.1. Using Absolute Time Range

Working Principle

When a time-based application enables a certain function, it determines whether current time is within the absolute time range. If yes, the function is effective or ineffective at the current time depending on specific configuration.

Related Configuration

→ Configuring Time Range

No time range is configured by default.

Use the **time-range** *time-range-name* command to configure a time range.

→ Configuring Absolute Time Range

The absolute time range is [00:00 January 1, 0, 23:59 December 31, 9999] by default.

Use the **absolute** { [start time date] | [end time date] } command to configure the absolute time range.

4.3.2. Using Periodic Time

Working Principle

When a time-based application enables a certain function, it determines whether current time is within the period time. If yes, the function is effective or ineffective at the current time depending on specific configuration.

Related Configuration

→ Configuring Time Range

No time range is configured by default.

Use the **time-range** *time-range-name* command to configure a time range.

→ Configure Periodic Time

No periodic time is configured by default.

Use the **periodic** *day-of-the-week time to [day-of-the-week] time* command to configure periodic time.

4.4. Configuration Details

Configuration Item	Suggestions and Related Commands	
<u>Configuring Time Range</u>	Mandatory configuration. Time range configuration is required so as to use the time range function.	
	time-range time-range-name	Configures a time range.
	Optional configuration. You can configure various parameters as necessary.	
	absolute { [start time date] [end time date] }	Configures an absolute time range.
	periodic day-of-the-week time to [day-of-the-week] time	Configures periodic time.

4.4.1. Configuring Time Range

Configuration Effect

- Configure a time range, which may be an absolute time range or a periodic time interval, so that a time-range-based application can enable a certain function within the time range.

Configuration Method

→ Configuring Time Range

- Mandatory configuration.
- Perform the configuration on a device to which a time range applies.

→ Configuring Absolute Time Range

- Optional configuration.

→ Configuring Periodic Time

- Optional configuration.

Verification

- Use the **show time-range** [*time-range-name*] command to check time range configuration information.

Related Commands

→ Configuring Time Range

Command Syntax	time-range <i>time-range-name</i>
Parameter Description	<i>time-range-name</i> : name of the time range to be created.
Command Mode	Global configuration mode
Usage Guide	Some applications (such as ACL) may run based on time. For example, an ACL can be effective within certain time ranges of a week. To this end, first you must configure a time range, then you can configure relevant time control in time range configuration mode.

→ Configuring Absolute Time Range

Command Syntax	absolute { [start <i>time date</i>] [end <i>time date</i>] }
Parameter Description	start <i>time date</i> : start time of the range. end <i>time date</i> : end time of the range.
Command Mode	Time range configuration mode
Usage Guide	Use the absolute command to configure a time absolute time range between a start time and an end time to allow a certain function to take effect within the absolute time range.

→ Configuring Periodic Time

Command Syntax	periodic <i>day-of-the-week time to</i> [<i>day-of-the-week</i>] <i>time</i>
Parameter Description	<i>day-of-the-week</i> : the week day when the periodic time starts or ends <i>time</i> : the exact time when the periodic time starts or ends
Command Mode	Time range configuration mode

**Usage
Guide**

Use the periodic command to configure a periodic time interval to allow a certain function to take effect within the periodic time.

4.5. Monitoring and Maintaining Time Range

Displaying the Running Status

Function	Command
Displays time range configuration.	show time-range [<i>time-range-name</i>]

5. CONFIGURING HTTP

5.1. Overview

Hypertext Transfer Protocol (HTTP) is used to transmit Web page information on the Internet. It is at the application layer of the TCP/IP protocol stack. The transport layer adopts connection-oriented Transmission Control Protocol (TCP).

Hypertext Transfer Protocol Secure (HTTPS) is an HTTP supporting the Secure Sockets Layer (SSL) protocol. HTTPS is mainly used to create a secure channel on an insecure network, ensure that information can hardly be intercepted, and provide certain reasonable protection against main-in-the-middle attacks. At present, HTTPS is widely used for secure and sensitive communication on the Internet, for example, electronic transactions.

Protocols and Standards

- RFC1945: Hypertext Transfer Protocol -- HTTP/1.0
- RFC2616: Hypertext Transfer Protocol -- HTTP/1.1
- RFC2818: Hypertext Transfer Protocol Over TLS -- HTTPS

5.2. Features

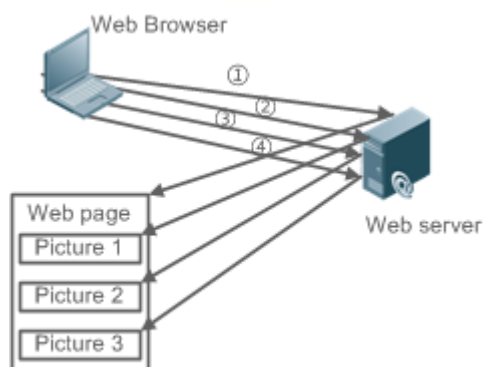
→ Basic Concepts

HTTP Service

The HTTP service refers to transmission of Web page information on the Internet by using HTTP. HTTP/1.0 is currently an HTTP version that is the most widely used. As one Web server may receive thousands or even millions of access requests, HTTP/1.0 adopts the short connection mode to facilitate connection management. One TCP connection is established for each request. After a request is completed, the TCP connection is released. The server does not need to record or trace previous requests. Although HTTP/1.0 simplifies connection management, HTTP/1.0 introduces performance defects.

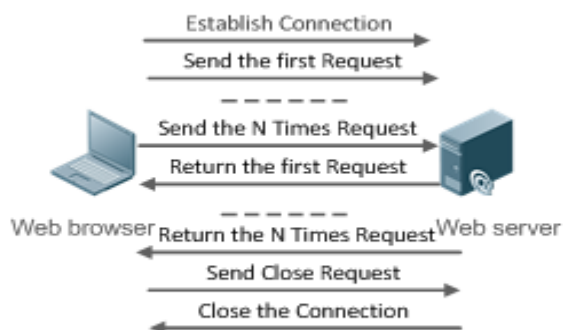
For example, a web page may need lots of pictures. However, the web page contains not real picture contents but URL connection addresses of the pictures. In this case, the browser sends multiple requests during access. Each request requires establishing an independent connection and each connection is completely isolated. Establishing and releasing connections is a relatively troublesome process, which severely affects the performance of the client and server, as shown in the following figure:

Figure 5-1



HTTP/1.1 overcomes the defect. It supports persistent connection, that is, one connection can be used to transmit multiple requests and response messages. In this way, a client can send a second request without waiting for completion of the previous request. This reduces network delay and improves performance. See the following figure:

Figure 5-2



At present, QTECH devices support both HTTP/1.0 and HTTP/1.1.

↳ Which HTTP version will be used by a device is decided by the Web browser.

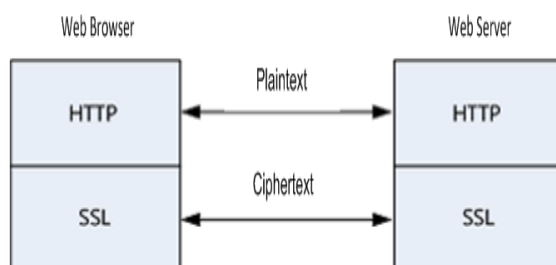
→ HTTPS Service

The HTTPS service adds the SSL based on the HTTP service. Its security basis is the SSL. To run HTTPS properly, a server must have a Public Key Infrastructure (PKI) certificate while a client may not necessarily need one. The SSL protocol provides the following services:

- Authenticating users and servers and ensuring that data is sent to the correct client and server.

- Encrypting data to prevent data from being stolen midway.
- Maintaining data integrity and ensuring that data is not changed during transmission.

Figure 5-3



→ HTTP Upgrade Service

- During a local upgrade, a device serves as an HTTP server. Users can log in to the device through a Web browser and upload upgrade files to the device to realize file upgrade on the device.

Features

Feature	Description
Local HTTP Upgrade Service	Upgrade files are uploaded to a device to realize file upgrade on the device.

5.2.1. Local HTTP Upgrade Service

When a device serves as the HTTP server, users can log in to the device through a Web browser and upload upgrade files (including component package and Web package) to the device or directly upload files to the device through Trivial File Transfer Protocol (TFTP).

Working Principle

- A component package or Web package is uploaded through the local upgrade function provided by Web.
- After successfully receiving a file, the device checks the version for its validity.
- After the file check is successful, if the file is a Web package, perform the upgrade directly; if the file is a component package, decide whether to perform the upgrade in the browser by restarting the device.

Related Configuration

→ Updating a Web Package

Run the **upgrade web download** command to download a Web package from the TFTP server. After the command is run, download a Web package from the TFTP server. After the package passes the validity check, directly use the Web package for upgrade without restarting the device.


You can also run the **upgrade web** command to directly upgrade a Web package stored locally.

→ Updating a Subsystem Component

By default, a device does not upgrade subsystem components uploaded through a browser or TFTP.

To upgrade a subsystem component, you must restart the device.

5.3. Configuration

Configuration	Description and Command
Configuring a Local HTTP Upgrade	 (Mandatory) It is used to realize a local HTTP upgrade.
	upgrade web Upgrades a Web package stored on a device.
	upgrade web download Automatically downloads a Web package from a server and automatically upgrades the package.

5.3.1. Configuring a Local HTTP Upgrade

Configuration Effect

Perform an HTTP upgrade through the browser or the upgrade web command.

Notes

- So long as a Web package is uploaded successfully and passes the version check, the device directly performs an upgrade based on the latest Web package.
- The upgrade **web download** command is used to automatically download files from the TFTP server and automatically perform an upgrade.
- The **upgrade web** command is used to automatically upgrade the Web package in the local file system.

Configuration Steps

N/A

Verification

- Access and view the latest Web page through the browser.

Related Commands

→ Downloading a Web Package from the TFTP Server


Command	upgrade web download { oob_tftp: /path tftp: /path }
Parameter Description	<i>oob_tftp</i> : Connects to the TFTP server through the management port and downloads a Web package. Only the devices that support the management port support the parameter. <i>tftp</i> : Connects the TFTP server through a common data port and downloads a Web package. <i>path</i> : Path of a Web package on the TFTP server.
Command Mode	Privileged mode
Usage Guide	This command is used to download a Web package from the TFTP server and automatically perform an upgrade.

→ Upgrading a Web Package Stored on a Local Device

Command	upgrade web uri
Parameter Description	<i>uri</i> : Local path for storing a Web package.
Command Mode	Privileged mode
Usage Guide	This command is used to upgrade a Web package stored on a device and automatically perform an upgrade.


Configuration Example

→ Obtaining the Latest Web Package from the Official Website and Running the Web Package


Scenario Figure 5-4	 <p>The diagram shows a network device labeled 'A' connected via a line to a laptop labeled 'Web browser'.</p>
Configuration Steps	<ul style="list-style-type: none"> ● Connect to a local PC whose IP address is 10.10.10.13 and assign an IP address 10.10.10.131 in the same network segment to the device. ● Log in to the device through Web and upload the latest Web package to the device.
A	<pre>A#configure terminal A(config)# vlan 1 A(config-vlan)# exit A(config)# interface vlan 1 A(config-VLAN 1)# ip address 10.10.10.131 255.255.255.0 A(config-VLAN 1)# exit</pre>

	A(config)# enable service web-server
	On a PC, use the local upgrade function on the Web page to upload a Web package for upgrade.
Verification	On the PC, log in to the device through Web again and check whether the latest Web page is displayed.

→ Upgrading a Web Package by Running the upgrade web download Command

Scenario Figure 5-5	
Configuration Steps	<ul style="list-style-type: none"> ● Connect to a local PC whose IP address is 10.10.10.13 and assign an IP address 10.10.10.131 in the same network segment to the device. ● Start the TFTP server.
A	<pre>A#configure terminal A(config)# vlan 1 A(config-vlan)# exit A(config)# interface vlan 1 A(config-VLAN 1)# ip address 10.10.10.131 255.255.255.0 A(config-VLAN 1)# end A#upgrade web download tftp:// 10.10.10.13/web.upd Press Ctrl+C to quit !!!!!!!!!! download 3896704 bytes Begin to upgrade the web package... Web package upgrade successfully.</pre>
Verification	On the PC, log in to the device through Web again and check whether the latest Web page is displayed.

→ Upgrading a Web Package by Running the upgrade web Command

Scenario Figure 5-6	
Configuration Steps	<ul style="list-style-type: none"> ● Connect to a local PC whose IP address is 10.10.10.13 and assign an IP address 10.10.10.131 in the same network segment to the device. ● Start the TFTP server.

A	<pre>A#configure terminal A(config)# vlan 1 A(config-vlan)# exit A(config)# interface vlan 1 A(config-VLAN 1)# ip address 10.10.10.131 255.255.255.0 A(config-VLAN 1)# end A#copy tftp://10.10.10.13/web.upd flash:/web.upd Press Ctrl+C to quit !!!!!!! Accessing tftp:// 10.10.10.13/web.upd finished, 3896704 bytes prepared Flushing data to flash:/web.upd... Flush data done A #upgrade web flash:/web.upd Web package upgrade successfully. A #</pre>
Verification	On the PC, log in to the device through Web again and check whether the latest Web page is displayed.

Common Errors

- Access to the web page through the browser shows that the web page is not updated based on the latest Web package. This is possibly because the local browser has a cache. Clear the cache of the local browser and access the Web page again.

6. CONFIGURING SYSLOG

6.1. Overview

Status changes (such as link up and down) or abnormal events may occur anytime. QTECH products provide the syslog mechanism to automatically generate messages (log packets) in fixed format upon status changes or occurrence of events. These messages are displayed on the related windows such as the Console or monitoring terminal, recorded on media such as the memory buffer or log files, or sent to a group of log servers on the network so that the administrator can analyze network performance and identify faults based on these log packets. Log packets can be added with the timestamps and sequence numbers and classified by severity level so that the administrator can conveniently read and manage log packets.

Protocols and Standards

- RFC3164: The BSD syslog Protocol

6.2. Applications

Application	Description
Sending Syslogs to the Console	Monitor syslogs through the Console.
Sending Syslogs to the Log Server	Monitor syslogs through the server.

6.2.1. Sending Syslogs to the Console

Scenario

Send syslogs to the Console to facilitate the administrator to monitor the performance of the system. The requirements are as follows:

1. Send logs of Level 6 or higher to the Console.
2. Send logs of only the ARP and IP modules to the Console.

Figure 6-1 shows the network topology.

Figure 6-1 Network topology



Deployment

Configure the device as follows:

1. Set the level of logs that can be sent to the Console to informational (Level 6).
2. Set the filtering direction of logs to terminal.
3. Set log filtering mode of logs to contains-only.
4. Set the filtering rule of logs to single-match. The module name contains only ARP or IP.

6.2.2. Sending Syslogs to the Log Server

Scenario

Send syslogs to the log server to facilitate the administrator to monitor the logs of devices on the server. The requirements are as follows:

1. Send syslogs to the log server 10.1.1.1.
2. Send logs of Level 7 or higher to the log server.
3. Send syslogs from the source interface Loopback 0 to the log server.

Figure 6-2 shows the network topology.

Figure 6-2 Network topology



Deployment

Configure the device as follows:

1. Set the IPv4 address of the server to 10.1.1.1.
2. Set the level of logs that can be sent to the log server to debugging (Level 7).
3. Set the source interface of logs sent to the log server to Loopback 0.

6.3. Features

Basic Concepts

→ Classification of Syslogs

Syslogs can be classified into two types:

- Log type
- Debug type

→ Levels of Syslogs

Eight severity levels of syslogs are defined in descending order, including emergency, alert, critical, error, warning, notification, informational, and debugging. These levels correspond to eight numerical values from 0 to 7. A smaller value indicates a higher level.

Only logs with a level equaling to or higher than the specified level can be output. For example, if the level of logs is set to informational (Level 6), logs of Level 6 or higher will be output.

The following table describes the log levels.

Level	Numerical Value	Description
emergencies	0	Indicates that the system cannot run normally.
alerts	1	Indicates that the measures must be taken immediately.
critical	2	Indicates a critical condition.
errors	3	Indicates an error.
warnings	4	Indicates a warning.
notifications	5	Indicates a notification message that requires attention.
informational	6	Indicates an informational message.
debugging	7	Indicates a debugging message.

→ Output Direction of Syslogs

Output directions of syslogs include Console, monitor, server, buffer, and file. The default level and type of logs vary with the output direction. You can customize filtering rules for different output directions.

The following table describes output directions of syslogs.

Output Direction	Description	Default Output Level	Description
Console	Console	Debugging (Level 7)	Logs and debugging information are output.
monitor	Monitoring terminal	Debugging (Level 7)	Logs and debugging information are output.
server	Log server	Informational (Level 6)	Logs and debugging information are output.
buffer	Log buffer	Debugging (Level 7)	Logs and debugging information are output. The log buffer is used to store syslogs.

file	Log file	Informational (Level 6)	Logs and debugging information are output. Logs in the log buffer are periodically written into files.
------	----------	-------------------------	--

→ RFC3164 Log Format

Formats of syslogs may vary with the syslog output direction.

- If the output direction is the Console, monitor, buffer, or file, the syslog format is as follows:

```
seq no: *timestamp: sysname %module-level-mnemonic: content
```

For example, if you exit configuration mode, the following log is displayed on the Console:

```
001233: *May 22 09:44:36: QTECH %SYS-5-CONFIG_I: Configured from console by console
```

- If the output direction is the log server, the syslog format is as follows:

```
<priority>seq no: *timestamp: sysname %module-level-mnemonic: content
```

For example, if you exit configuration mode, the following log is displayed on the log server:

```
<189>001233: *May 22 09:44:36: QTECH %SYS-5-CONFIG_I: Configured from console by console
```

The following describes each field in the log in details:

4. Priority

This field is valid only when logs are sent to the log server.

The priority is calculated using the following formula: Facility x 8 + Level. Level indicates the numerical code of the log level and Facility indicates the numerical code of the facility. The default facility value is local7 (23). The following table lists the value range of the facility.

Numerical Code	Facility Keyword	Facility Description
0	kern	kernel messages
1	user	user-level messages
2	mail	mail system
3	daemon	system daemons
4	auth1	security/authorization messages
5	syslog	messages generated internally by syslogs
6	lpr	line printer subsystem
7	news	network news subsystem
8	uucp	UUCP subsystem
9	clock1	clock daemon

10	auth2	security/authorization messages
11	ftp	FTP daemon
12	ntp	NTP subsystem
13	logaudit	log audit
14	logalert	log alert
15	clock2	clock daemon
16	local0	local use 0 (local0)
17	local1	local use 1 (local1)
18	local2	local use 2 (local2)
19	local3	local use 3 (local3)
20	local4	local use 4 (local4)
21	local5	local use 5 (local5)
22	local6	local use 6 (local6)
23	local7	local use 7 (local7)

5. Sequence Number

The sequence number of a syslog is a 6-digit integer, and increases sequentially. By default, the sequence number is not displayed. You can run a command to display or hide this field.

6. Timestamp

The timestamp records the time when a syslog is generated so that you can display and check the system event conveniently. QTECH devices support two syslog timestamp formats: datetime and uptime.

⚠ If the device does not have the real time clock (RTC), which is used to record the system absolute time, the device uses its startup time (uptime) as the syslog timestamp by default. If the device has the RTC, the device uses its absolute time (datetime) as the syslog timestamp by default.

The two timestamp formats are described as follows:

- Datetime format

The datetime format is as follows:

```
Mmm dd yyyy hh:mm:ss.msec
```

The following table describes each parameter of the datetime.

Timestamp Parameter	Parameter Name	Description
Mmm	Month	Mmm refers to abbreviation of the current month. The 12 months in a year are written as Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec.
dd	Day	dd indicates the current date.
yyyy	Year	yyyy indicates the current year, and is not displayed by default.
hh	Hour	hh indicates the current hour.
mm	Minute	mm indicates the current minute.
ss	Second	ss indicates the current second.
msec	Millisecond	msec indicates the current millisecond.

By default, the datetime timestamp displayed in the syslog does not contain the year and millisecond. You can run a command to display or hide the year and millisecond of the datetime timestamp.

- Uptime format

The uptime format is as follows:

```
dd:hh:mm:ss
```

The timestamp string indicates the accumulated days, hours, minutes, and seconds since the system is started.

7. Sysname

This field indicates the name of the device that generates the log so that the log server can identify the host that sends the log. By default, this field is not displayed. You can run a command to display or hide this field.

8. Module

This field indicates the name of the module that generates the log. The module name is an upper-case string of 2 to 20 characters, which contain upper-case letters, digits, or underscores. The module field is mandatory in the log-type information, and optional in the debug-type information.

9. Level

Eight syslog levels from 0 to 7 are defined. The level of syslogs generated by each module is fixed and cannot be modified.

10. Mnemonic

This field indicates the brief information about the log. The mnemonic is an upper-case string of 4 to 32 characters, which may include upper-case letters, digits, or underscore. The mnemonic field is mandatory in the log-type information, and optional in the debug-type information.

11. Content

This field indicates the detailed content of the syslog.

Overview

Feature	Description
Logging	Enable or disable the system logging functions.
Syslog Format	Configure the syslog format.
Logging Direction	Configure the parameters to send syslogs in different directions.
Syslog Filtering	Configure parameters of the syslog filtering function.
Featured Logging	Configure parameters of the featured logging function.
Syslog Monitoring	Configure parameters of the syslog monitoring function.

6.3.1. Logging

Enable or disable the logging, log redirection, and log statistics functions.

Related Configuration

→ Enable Logging

By default, logging is enabled.

Run the **logging on** command to enable logging in global configuration mode. After logging is enabled, logs generated by the system are sent in various directions for the administrator to monitor the performance of the system.

→ Enabling Log Redirection

By default, log redirection is enabled on the Virtual Switching Unit (VSU).

Run the **logging rd on** command to enable log redirection in global configuration mode. After log redirection is enabled, logs generated by the standby device or standby supervisor module are redirected to the active device or active supervisor module on the VSU to facilitate the administrator to manage logs.

→ Enabling Log Statistics

By default, log statistics is disabled.

Run the **logging count** command to enable log statistics in global configuration mode. After log statistics is enabled, the system records the number of times a log is generated and the last time when the log is generated.

6.3.2. Syslog Format

Configure the syslog format, including the RFC5424 log format, timestamp format, sysname, and sequence number.

Related Configuration

→ Configuring the Timestamp Format

By default, the syslog uses the datetime timestamp format, and the timestamp does not contain the year and millisecond.

Run the **service timestamps** command in global configuration mode to use the datetime timestamp format that contains the year and millisecond in the syslog, or change the datetime format to the uptime format.

→ Adding Sysname to the Syslog

By default, the syslog does not contain sysname.

Run the **service sysname** command in global configuration mode to add sysname to the syslog.

→ Adding the Sequence Number to the Syslog

By default, the syslog does not contain the sequence number.

Run the **service sequence-numbers** command in global configuration mode to add the sequence number to the syslog.

→ Enabling the Standard Log Format

By default, logs are displayed in the following format:

```
*timestamp: %module-level-mnemonic: content
```

Run the **service standard-syslog** command in global configuration mode to enable the standard log format and logs are displayed in the following format:

```
timestamp %module-level-mnemonic: content
```

Compared with the default log format, an asterisk (*) is missing in front of the timestamp, and a colon (:) is missing at the end of the timestamp in the standard log format.

→ Enabling the Private Log Format

By default, logs are displayed in the following format:

```
*timestamp: %module-level-mnemonic: content
```

Run the **service private-syslog** command in global configuration mode to enable the private log format and logs are displayed in the following format:

```
timestamp module-level-mnemonic: content
```

Compared with the default log format, an asterisk (*) is missing in front of the timestamp, a colon (:) is missing at the end of the timestamp, and a percent sign (%) is missing at the end of the module name in the private log format.

6.3.3. Logging Direction

Configure parameters for sending syslogs in different directions, including the Console, monitor terminal, buffer, the log server, and log files.

Related Configuration

→ Synchronizing User Input with Log Output

By default, this function is disabled.

Run the **logging synchronous** command in line configuration mode to synchronize user input with log output. After this function is enabled, user input will not be interrupted.

→ Configuring the Log Rate Limit

By default, no log rate limit is configured.

Run the **logging rate-limit** { *number* | **all** *number* | **console** {*number* | **all** *number* } } [**except** [*severity*]] command in global configuration mode to configure the log rate limit.

→ Configuring the Log Redirection Rate Limit

By default, a maximum of 200 logs are redirected from the standby device to the active device of VSU per second.

Run the **logging rd rate-limit** *number* [**except** *severity*] command in global configuration mode to configure the log redirection rate limit, that is, the maximum number of logs that are redirected from the standby device to the active device or from the standby supervisor module to the active supervisor module per second.

→ Configuring the Level of Logs Sent to the Console

By default, the level of logs sent to the Console is debugging (Level 7).

Run the **logging console** [*level*] command in global configuration mode to configure the level of logs that can be sent to the Console.

→ Sending Logs to the Monitor Terminal

By default, it is not allowed to send logs to the monitor terminal.

Run the terminal monitor command in the privileged EXEC mode to send logs to the monitor terminal.

→ Configuring the Level of Logs Sent to the Monitor Terminal

By default, the level of logs sent to the monitor terminal is debugging (Level 7).

Run the **logging monitor** [*level*] command in global configuration mode to configure the level of logs that can be sent to the monitor terminal.

→ Writing Logs into the Memory Buffer

By default, logs are written into the memory buffer, and the default level of logs is debugging (Level 7).

Run the **logging buffered** [*buffer-size*] [*level*] command in global configuration mode to configure parameters for writing logs into the memory buffer, including the buffer size and log level.

→ Sending Logs to the Log Server

By default, logs are not sent to the log server.

Run the **logging server** [*oob*] { *ip-address* | **ipv6** *ipv6-address* } [**via** *mgmt-name*] [**udp-port** *port*] [**vrf** *vrf-name*] command in global configuration mode to send logs to a specified log server.

→ Configuring the Level of Logs Sent to the Log Server

By default, the level of logs sent to the log server is informational (Level 6).

Run the **logging trap** [*level*] command in global configuration mode to configure the level of logs that can be sent to the log server.

→ Configuring the Facility Value of Logs Sent to the Log Server

If the RFC5424 log format is disabled, the facility value of logs sent to the log server is local7 (23) by default. If the RFC5424 log format is enabled, the facility value of logs sent to the log server is local0 (16) by default.

Run the **logging facility** *facility-type* command in global configuration mode to configure the facility value of logs sent to the log server.

→ Configuring the Source Address of Logs Sent to the Log Server

By default, the source address of logs sent to the log server is the IP address of the interface sending logs.

Run the **logging source** [**interface**] *interface-type interface-number* command to configure the source interface of logs. If this source interface is not configured, or the IP address is not

configured for this source interface, the source address of logs is the IP address of the interface sending logs.

Run the **logging source** { **ip** *ip-address* | **ipv6** *ipv6-address* } command to configure the source IP address of logs. If this IP address is not configured on the device, the source address of logs is the IP address of the interface sending logs.

→ Writing Logs into Log Files

By default, logs are not written into log files. After the function of writing logs into log files is enabled, the level of logs written into log files is informational (Level 6) by default.

Run the **logging file** { **flash:filename** | **usb0:filename** | **usb1:filename** } [*max-file-size*] [*level*] command in global configuration mode to configure parameters for writing logs into log files, including the type of device where the file is stored, file name, file size, and log level.

→ Configuring the Interval at Which Logs Are Written into Log Files

By default, logs are written into log files at the interval of 3600s (one hour).

Run the **logging flash interval** *seconds* command in global configuration mode to configure the interval at which logs are written into log files.

→ Configuring the Storage Time of Log Files

By default, the storage time is not configured.

Run the **logging life-time level** *level* *days* command in global configuration mode to configure the storage time of logs. The administrator can specify different storage days for logs of different levels.

→ Immediately Writing Logs in the Buffer into Log Files

By default, syslog messages are stored in the syslog buffer and then written into log files periodically or when the buffer is full.

Run the **logging flash flush** command in global configuration mode to immediately write logs in the buffer into log files so that you can collect logs conveniently.

6.3.4. Syslog Filtering

By default, logs generated by the system are sent in all directions.

Working Principle

→ Filtering Direction

Five log filtering directions are defined:

- **buffer**: Filters out logs sent to the log buffer, that is, logs displayed by the show logging command.

- **file:** Filters out logs written into log files.
- **server:** Filters out logs sent to the log server.
- **terminal:** Filters out logs sent to the Console and monitor terminal (including Telnet and SSH).

The four filtering directions can be used either in combinations to filter out logs sent in various directions, or separately to filter out logs sent in a single direction.

→ Filtering Mode

Two filtering modes are available:

- **contains-only:** Indicates that only logs that contain keywords specified in the filtering rules are output. You may be interested in only a specified type of logs. In this case, you can apply the contains-only mode on the device to display only logs that match filtering rules on the terminal, helping you check whether any event occurs.
- **filter-only:** Indicates that logs that contain keywords specified in the filtering rules are filtered out and will not be output. If a module generates too many logs, spamming may occur on the terminal interface. If you do not care about this type of logs, you can apply the filter-only mode and configure related filtering rules to filter out logs that may cause spamming.

The two filtering modes are mutually exclusive, that is, you can configure only one filtering mode at a time.

→ Filter Rule

Two filtering rules are available:

- **exact-match:** If exact-match is selected, you must select all the three filtering options (module, level, and mnemonic). If you want to filter out a specified log, use the exact-match filtering rule.
- **single-match:** If exact-match is selected, you only need to select one of the three filtering options (module, level, and mnemonic). If you want to filter out a specified type of logs, use the single-match filtering rule.

If the same module, level, or mnemonic is configured in both the single-match and exact-match rules, the single-match rule prevails over the exact-match rule.

Related Configuration

→ Configuring the Log Filtering Direction

By default, the log filtering direction is all, that is, logs sent in all directions are filtered.

Run the **logging filter direction** { **all** | **buffer** | **file** | **server** | **terminal** } command in global configuration mode to configure the log filtering direction to filter out logs in the specified directions.

→ Configuring the Log Filtering Mode

By default, the log filtering mode is filter-only.

Run the **logging filter type** { **contains-only** | **filter-only** } command in global configuration mode to configure the log filtering mode.

→ Configuring the Log Filtering Rule

By default, no log filtering rule is configured on a device, that is, logs are not filtered out.

Run the **logging filter rule exact-match module** *module-name mnemonic mnemonic-name level level* command in global configuration mode to configure the exact-match rule.

Run the **logging filter rule single-match** { **level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name* } command in global configuration mode to configure the single-match rule.

6.3.5. Syslog Monitoring

After syslog monitoring is enabled, the system monitors the access attempts of users and generates the related logs.

Working Principle

After logging of login/exit attempts is enabled, the system records the access attempts of users. The log contains user name and source address.

After logging of operations is enabled, the system records changes in device configurations. The log contains user name, source address, and operation.

Related Configuration

→ Enabling Logging of Login or Exit Attempts

By default, a device does not generate logs when users access or exit the device.






Run the **logging userinfo** command in global configuration mode to enable logging of login/exit attempts. After this function is enabled, the device displays logs when users access the devices through Telnet, SSH, or HTTP so that the administrator can monitor the device connections.

→ Enabling Logging of Operations

By default, a device does not generate logs when users modify device configurations.

Run the **logging userinfo command-log** command in global configuration mode to enable logging of operations. After this function is enabled, the system displays related logs to notify the administrator of configuration changes.

6.4. Configuration

Configuration	Description and Command
Configuring Syslog Format	 (Optional) It is used to configure the syslog format.
	service timestamps [message-type [uptime datetime [msec] [year]]] Configures the timestamp format of syslogs.
	service sysname Adds the sysname to the syslog.
	service sequence-numbers Adds the sequence number to the syslog.
	service standard-syslog Enables the standard syslog format.
	service private-syslog Enables the private syslog format.
Sending Syslogs to the Console	 (Optional) It is used to configure parameters for sending syslogs to the Console.
	logging on Enables logging.
	logging count Enables log statistics.
	logging console [level] Configures the level of logs displayed on the Console.
	logging rate-limit { number all number console { number all number } } [except [severity]] Configures the log rate limit.
Sending Syslogs to the Monitor Terminal	 (Optional) It is used to configure parameters for sending syslogs to the monitor terminal.
	terminal monitor Enables the monitor terminal to display logs.
	logging monitor [level] Configures the level of logs displayed on the monitor terminal.
Writing Syslogs into the Memory Buffer	 (Optional) It is used to configure parameters for writing syslogs into the memory buffer.
	logging buffered [buffer-size] [level] Configures parameters for writing syslogs into the memory buffer, including the buffer size and log level.
Sending Syslogs to the Log Server	 (Optional) It is used to configure parameters for sending syslogs to the log server.

	logging server [oob] { <i>ip-address</i> ipv6 <i>ipv6-address</i> } [via <i>mgmt-name</i>] [udp-port <i>port</i>] [vrf <i>vrf-name</i>]	Sends logs to a specified log server.
	logging trap [<i>level</i>]	Configures the level of logs sent to the log server.
	logging facility <i>facility-type</i>	Configures the facility value of logs sent to the log server.
	logging source [interface] <i>interface-type interface-number</i>	Configures the source interface of logs sent to the log server.
	logging source { ip <i>ip-address</i> ipv6 <i>ipv6-address</i> }	Configures the source address of logs sent to the log server.
<u>Writing Syslogs into Log Files</u>	<p>👉 (Optional) It is used to configure parameters for writing syslogs into a file.</p>	
	logging file { flash : <i>filename</i> usb0 : <i>filename</i> usb1 : <i>filename</i> } [<i>max-file-size</i>] [<i>level</i>]	Configures parameters for writing syslogs into a file, including the file storage type, file name, file size, and log level.
	logging flash interval <i>seconds</i>	Configures the interval at which logs are written into log files. The default value is 3600.
	logging life-time level <i>level days</i>	Configures the storage time of log files.
<u>Configuring Syslog Filtering</u>	<p>👉 (Optional) It is used to enable the syslog filtering function.</p>	
	logging filter direction { all buffer file server terminal }	Configures the log filtering direction.
	logging filter type { contains-only filter-only }	Configures the log filtering mode.
	logging filter rule exact-match module <i>module-name mnemonic mnemonic-name level level</i>	Configures the exact-match filtering rule.
	logging filter rule single-match { <i>level level</i> mnemonic <i>mnemonic-name</i> module <i>module-name</i> }	Configures the single-match filtering rule.
<u>Configuring Syslog Redirection</u>	<p>👉 (Optional) It is used to enable the log redirection function.</p>	
	logging rd on	Enables the log redirection function.
	logging rd rate-limit <i>number</i> [except severity]	Configures the log redirection rate limit.

<u>Configuring Syslog Monitoring</u>	<p>☞ (Optional) It is used to configure parameters of the syslog monitoring function.</p>	
	logging userinfo	Enables logging of login/exit attempts.
	logging userinfo command-log	Enables logging of operations.
<u>Synchronizing User Input with Log Output</u>	<p>☞ (Optional) It is used to synchronize the user input with log output.</p>	
	logging synchronous	Synchronizes user input with log output.

6.4.1. Configuring Syslog Format

Configuration Effect

- Configure the format of syslogs.

Notes

→ RFC3164 Log Format

- If the device does not have the real time clock (RTC), which is used to record the system absolute time, the device uses its startup time (uptime) as the syslog timestamp by default. If the device has the RTC, the device uses its absolute time (datetime) as the syslog timestamp by default.
- The log sequence number is a 6-digit integer. Each time a log is generated, the sequence number increases by one. Each time the sequence number increases from 000000 to 1,000,000, or reaches 2^{32} , the sequence number starts from 000000 again.

Configuration Steps

→ Configuring the Timestamp Format of Syslogs

- (Optional) By default, the datetime timestamp format is used.
- Unless otherwise specified, perform this configuration on the device to configure the timestamp format.

→ Adding the Sysname to the Syslog

- (Optional) By default, the syslog does not contain the sysname.
- Unless otherwise specified, perform this configuration on the device to add the sysname to the syslog.

→ Adding the Sequence Number to the Syslog

- (Optional) By default, the syslog does not contain the sequence number.
- Unless otherwise specified, perform this configuration on the device to add the sequence number to the syslog.

→ Enabling the Standard Log Format

- (Optional) By default, the default log format is used.
- Unless otherwise specified, perform this configuration on the device to enable the standard log format.

→ Enabling the Private Log Format

- (Optional) By default, the default log format is used.
- Unless otherwise specified, perform this configuration on the device to enable the private log format.

Verification

- Generate a syslog, and check the log format.

Related Commands

→ Configuring the Timestamp Format of Syslogs

Command	service timestamps [<i>message-type</i> [uptime datetime [msec] [year]]
Parameter Description	<i>message-type</i> : Indicates the log type. There are two log types: log and debug. uptime : Indicates the device startup time in the format of dd:hh:mm:ss, for example, 07:00:10:41. datetime : Indicates the current device time in the format of MM DD hh:mm:ss, for example, Jul 27 16:53:07. msec : Indicates that the current device time contains millisecond. year : Indicates that the current device time contains year.
Command Mode	Global configuration mode
Configuration Usage	Two syslog timestamp formats are available, namely, uptime and datetime. You can select a timestamp format as required.

→ Adding the Sysname to the Syslog

Command	service sysname
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	This command is used to add the sysname to the log to enable you to learn about the device that sends syslogs to the server.

→ Adding the Sequence Number to the Syslog

Command	service sequence-numbers
Parameter Description	N/A

Command Mode	Global configuration mode
Configuration Usage	This command is used to add the sequence number to the log. The sequence number starts from 1. After the sequence number is added, you can learn clearly whether any log is lost and the generation sequence of logs.

→ Enabling the Standard Syslog Format

Command	service standard-syslog
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	<p>By default, logs are displayed in the following format (default format):</p> <pre>*timestamp: %module-level-mnemonic: content</pre> <p>If the standard syslog format is enabled, logs are displayed in the following format:</p> <pre>timestamp %module-level-mnemonic: content</pre> <p>Compared with the default format, an asterisk (*) is missing in front of the timestamp, and a colon (:) is missing at the end of the timestamp in the standard log format.</p>

→ Enabling the Private Syslog Format

Command	service private-syslog
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	<p>By default, logs are displayed in the following format (default format):</p> <pre>*timestamp: %module-level-mnemonic: content</pre> <p>If the private syslog format is enabled, logs are displayed in the following format:</p> <pre>timestamp module-level-mnemonic: content</pre> <p>Compared with the default format, an asterisk (*) is missing in front of the timestamp, a colon (:) is missing at the end of the timestamp, and a percent sign (%) is missing in front of the module name in the private log format.</p>

Configuration Example

→ Enabling the RFC3164 Log Format

Scenario	<p>It is required to configure the timestamp format as follows:</p> <ol style="list-style-type: none"> 1. Enable the RFC3164 format. 2. Change the timestamp format to datetime and add the millisecond and year to the timestamp. 3. Add the sysname to the log. 4. Add the sequence number to the log.
-----------------	--

Configuration Steps	<ul style="list-style-type: none">● Configure the syslog format.
	<pre>QTECH# configure terminal QTECH(config)# no service log-format rfc5424 QTECH(config)# service timestamps log datetime year msec QTECH(config)# service timestamps debug datetime year msec QTECH(config)# service sysname QTECH(config)# service sequence-numbers</pre>
Verification	<p>After the timestamp format is configured, verify that new syslogs are displayed in the RFC3164 format.</p> <ul style="list-style-type: none">● Run the show logging config command to display the configuration.● Enter or exit global configuration mode to generate a new log, and check the format of the timestamp in the new log.
	<pre>QTECH(config)#exit 001302: *Jun 14 2013 19:01:40.293: QTECH %SYS-5-CONFIG_I: Configured from console by admin on console QTECH#show logging config Syslog logging: enabled Console logging: level informational, 1306 messages logged Monitor logging: level informational, 0 messages logged Buffer logging: level informational, 1306 messages logged File logging: level informational, 121 messages logged File name:syslog_test.txt, size 128 Kbytes, have written 5 files Standard format:false Timestamp debug messages: datetime Timestamp log messages: datetime Sequence-number log messages: enable Sysname log messages: enable Count log messages: enable Trap logging: level informational, 121 message lines logged,0 fail</pre>

6.4.2. Sending Syslogs to the Console

Configuration Effect

- Send syslogs to the Console to facilitate the administrator to monitor the performance of the system.

Notes

- If too many syslogs are generated, you can limit the log rate to reduce the number of logs displayed on the Console.

Configuration Steps

→ Enabling Logging

- (Optional) By default, the logging function is enabled.

→ Enabling Log Statistics

- (Optional) By default, log statistics is disabled.
- Unless otherwise specified, perform this configuration on the device to enable log statistics.

→ Configuring the Level of Logs Displayed on the Console

- (Optional) By default, the level of logs displayed on the Console is debugging (Level 7).
- Unless otherwise specified, perform this configuration on the device to configure the level of logs displayed on the Console.

→ Configuring the Log Rate Limit

- (Optional) By default, the no rate limit is configured.
- Unless otherwise specified, perform this configuration on the device to limit the log rate.

Verification

- Run the show logging config command to display the level of logs displayed on the Console.

Related Commands

→ Enabling Logging

Command	logging on
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	By default, logging is enabled. Do not disable logging in general cases. If too many syslogs are generated, you can configure log levels to reduce the number of logs.

→ Enabling Log Statistics

Command	logging count
Parameter Description	N/A
Command Mode	Global configuration mode

Configurati on Usage	By default, log statistics is disabled. If log statistics is enabled, syslogs will be classified and counted. The system records the number of times a log is generated and the last time when the log is generated.
---------------------------------	--

→ Configuring the Level of Logs Displayed on the Console

Command	logging console [<i>level</i>]
Parameter Description	level: Indicates the log level.
Command Mode	Global configuration mode
Configurati on Usage	By default, the level of logs displayed on the Console is debugging (Level 7). You can run the show logging config command in privileged EXEC mode to display the level of logs displayed on the Console.

→ Configuring the Log Rate Limit

Command	logging rate-limit { <i>number</i> all <i>number</i> console { <i>number</i> all <i>number</i> } } [except [<i>severity</i>]]
Parameter Description	<i>number</i> : Indicates the maximum number of logs processed per second. The value ranges from 1 to 10,000. all : Indicates that rate limit is applied to all logs ranging from Level 0 to Level 7. console : Indicates the number of logs displayed on the Console per second. except severity : Rate limit is not applied to logs with a level equaling to or lower than the specified severity level. By default, the severity level is error (Level 3), that is, rate limit is not applied to logs of Level 3 or lower.
Command Mode	Global configuration mode
Configurati on Usage	By default, no rate limit is configured.

Configuration Example

→ Sending Syslogs to the Console

Scenario	It is required to configure the function of displaying syslogs on the Console as follows: 1. Enable log statistics. 2. Set the level of logs that can be displayed on the Console to informational (Level 6). 3. Set the log rate limit to 50.
Configurati on Steps	<ul style="list-style-type: none"> ● Configure parameters for displaying syslogs on the Console. <pre>QTECH# configure terminal QTECH(config)# logging count QTECH(config)# logging console informational QTECH(config)# logging rate-limit console 50</pre>

Verification	<ul style="list-style-type: none">● Run the show logging config command to display the configuration.
	<pre>QTECH(config)#show logging config Syslog logging: enabled Console logging: level informational, 1303 messages logged Monitor logging: level debugging, 0 messages logged Buffer logging: level debugging, 1303 messages logged File logging: level informational, 118 messages logged File name:syslog_test.txt, size 128 Kbytes, have written 5 files Standard format:false Timestamp debug messages: datetime Timestamp log messages: datetime Sequence-number log messages: enable Sysname log messages: enable Count log messages: enable Trap logging: level informational, 118 message lines logged,0 fail</pre>

6.4.3. Sending Syslogs to the Monitor Terminal

Configuration Effect

- Send syslogs to a remote monitor terminal to facilitate the administrator to monitor the performance of the system.

Notes

- If too many syslogs are generated, you can limit the log rate to reduce the number of logs displayed on the monitor terminal.
- By default, the current monitor terminal is not allowed to display logs after you access the device remotely. You need to manually run the terminal monitor command to allow the current monitor terminal to display logs.

Configuration Steps

→ Allowing the Monitor Terminal to Display Logs

- (Mandatory) By default, the monitor terminal is not allowed to display logs.
- Unless otherwise specified, perform this operation on every monitor terminal connected to the device.

→ Configuring the Level of Logs Displayed on the Monitor Terminal

- (Optional) By default, the level of logs displayed on the monitor terminal is debugging (Level 7).

- Unless otherwise specified, perform this configuration on the device to configure the level of logs displayed on the monitor terminal.

Verification

- Run the show logging config command to display the level of logs displayed on the monitor terminal.

Related Commands

→ Allowing the Monitor Terminal to Display Logs

Command	terminal monitor
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Configuration Usage	By default, the current monitor terminal is not allowed to display logs after you access the device remotely. You need to manually run the terminal monitor command to allow the current monitor terminal to display logs.

→ Configuring the Level of Logs Displayed on the Monitor Terminal

Command	logging monitor [level]
Parameter Description	<i>level</i> : Indicates the log level.
Command Mode	Global configuration mode
Configuration Usage	By default, the level of logs displayed on the monitor terminal is debugging (Level 7). You can run the show logging config command in privileged EXEC mode to display the level of logs displayed on the monitor terminal.

Configuration Example

→ Sending Syslogs to the Monitor Terminal

Scenario	It is required to configure the function of displaying syslogs on the monitor terminal as follows: <ol style="list-style-type: none"> 1. Display logs on the monitor terminal. 2. Set the level of logs that can be displayed on the monitor terminal to informational (Level 6).
Configuration Steps	<ul style="list-style-type: none"> • Configure parameters for displaying syslogs on the monitor terminal.
	<pre>QTECH# configure terminal QTECH(config)# logging monitor informational QTECH(config)# line vty 0 4 QTECH(config-line)# monitor</pre>

Verification	<ul style="list-style-type: none">● Run the show logging config command to display the configuration.
	<pre>QTECH#show logging config Syslog logging: enabled Console logging: level informational, 1304 messages logged Monitor logging: level informational, 0 messages logged Buffer logging: level debugging, 1304 messages logged File logging: level informational, 119 messages logged File name:syslog_test.txt, size 128 Kbytes, have written 5 files Standard format:false Timestamp debug messages: datetime Timestamp log messages: datetime Sequence-number log messages: enable Sysname log messages: enable Count log messages: enable Trap logging: level informational, 119 message lines logged,0 fail</pre>

Common Errors

- To disable this function, run the terminal no monitor command, instead of the no terminal monitor command.

6.4.4. Writing Syslogs into the Memory Buffer

Configuration Effect

- Write syslogs into the memory buffer so that the administrator can view recent syslogs by running the show logging command.

Notes

- If the buffer is full, old logs will be overwritten by new logs that are written into the memory buffer.

Configuration Steps

→ Writing Logs into the Memory Buffer

- (Optional) By default, the system writes logs into the memory buffer, and the default level of logs is debugging (Level 7).
- Unless otherwise specified, perform this configuration on the device to write logs into the memory buffer.

Verification

- Run the **show logging config** command to display the level of logs written into the memory buffer.

- Run the **show logging** command to display the level of logs written into the memory buffer.

Related Commands

→ Writing Logs into the Memory Buffer

Command	logging buffered [<i>buffer-size</i>] [<i>level</i>]
Parameter Description	<i>buffer-size</i> : Indicates the size of the memory buffer. <i>level</i> : Indicates the level of logs that can be written into the memory buffer.
Command Mode	Global configuration mode
Configuration Usage	By default, the level of logs written into the memory buffer is debugging (Level 7). Run the show logging command in privileged EXEC mode to display the level of logs written into the memory buffer and the buffer size.

Configuration Example

→ Writing Syslogs into the Memory Buffer

Scenario	It is required to configure the function of writing syslog into the memory buffer as follows: 1. Set the log buffer size to 128 KB (131,072 bytes). 2. Set the information level of logs that can be written into the memory buffer to informational (Level 6).
Configuration Steps	<ul style="list-style-type: none"> ● Configure parameters for writing syslog into the memory buffer. <pre>QTECH# configure terminal QTECH(config)# logging buffered 131072 informational</pre>
Verification	<ul style="list-style-type: none"> ● Run the show logging config command to display the configuration and recent syslogs. <pre>QTECH#show logging Syslog logging: enabled Console logging: level informational, 1306 messages logged Monitor logging: level informational, 0 messages logged Buffer logging: level informational, 1306 messages logged File logging: level informational, 121 messages logged File name:syslog_test.txt, size 128 Kbytes, have written 5 files Standard format:false Timestamp debug messages: datetime Timestamp log messages: datetime Sequence-number log messages: enable Sysname log messages: enable</pre>

```
Count log messages: enable
Trap logging: level informational, 121 message lines logged,0 fail
Log Buffer (Total 131072 Bytes): have written 4200
001301: *Jun 14 2013 19:01:09.488: QTECH %SYS-5-CONFIG_I: Configured
from console by admin on console
001302: *Jun 14 2013 19:01:40.293: QTECH %SYS-5-CONFIG_I: Configured
from console by admin on console
//Logs displayed are subject to the actual output of the show logging
command.
```

6.4.5. Sending Syslogs to the Log Server

Configuration Effect

- Send syslogs to the log server to facilitate the administrator to monitor logs on the server.

Notes

- If the device has a MGMT interface and is connected to the log server through the MGMT interface, you must add the oob option (indicating that syslogs are sent to the log server through the MGMT interface) when configuring the logging server command.
- To send logs to the log server, you must add the timestamp and sequence number to logs. Otherwise, the logs are not sent to the log server.

Configuration Steps

→ Sending Logs to a Specified Log Server

- (Mandatory) By default, syslogs are not sent to any log server.
- Unless otherwise specified, perform this configuration on every device.

→ Configuring the Level of Logs Sent to the Log Server

- (Optional) By default, the level of logs sent to the log server is informational (Level 6).
- Unless otherwise specified, perform this configuration on the device to configure the level of logs sent to the log server.

→ Configuring the Facility Value of Logs Sent to the Log Server

- (Optional) If the RFC5424 format is disabled, the facility value of logs sent to the log server is local7 (23) by default. If the RFC5424 format is enabled, the facility value of logs sent to the log server is local0 (16) by default.
- Unless otherwise specified, perform this configuration on the device to configure the facility value of logs sent to the log server.

→ Configuring the Source Interface of Logs Sent to the Log Server

- (Optional) By default, the source interface of logs sent to the log server is the interface sending the logs.

- Unless otherwise specified, perform this configuration on the device to configure the source interface of logs sent to the log server.

→ Configuring the Source Address of Logs Sent to the Log Server

- (Optional) By default, the source address of logs sent to the log server is the IP address of the interface sending the logs.
- Unless otherwise specified, perform this configuration on the device to configure the source address of logs sent to the log server.

Verification

- Run the **show logging config** command to display the configurations related to the log server.

Related Commands

→ Sending Logs to a Specified Log Server

Command	logging server [oob] { <i>ip-address</i> ipv6 <i>ipv6-address</i> } [via <i>mgmt-name</i>] [udp-port <i>port</i>] [vrf <i>vrf-name</i>] Or logging { <i>ip-address</i> ipv6 <i>ipv6-address</i> } [udp-prot <i>port</i>] [vrf <i>vrf-name</i>]
Parameter Description	oob : Indicates that logs are sent to the log server through the MGMT interface. <i>ip-address</i> : Specifies the IP address of the host that receives logs. ipv6 <i>ipv6-address</i> : Specifies the IPv6 address of the host that receives logs. via <i>mgmt-name</i> : Specifies the MGMT interface used by the log server when the oob option is included in the command. vrf <i>vrf-name</i> : Specifies the VPN routing and forwarding (VRF) instance connected to the log server. udp-port <i>port</i> : Specifies the port ID of the log server. The default port ID is 514.
Command Mode	Global configuration mode
Configuration Usage	This command is used to specify the address of the log server that receives logs. You can specify multiple log servers, and logs will be sent simultaneously to all these log servers. 👉 You can specify via only when oob is included in the command. In this case, vrf cannot be used. 👉 You can configure up to five log servers on a QTECH product.

→ Configuring the Level of Logs Sent to the Log Server

Command	logging trap [<i>level</i>]
Parameter Description	<i>level</i> : Indicates the log level.
Command Mode	Global configuration mode
Configuration Usage	By default, the level of logs sent to the log server is informational (Level 6).

	You can run the show logging config command in privileged EXEC mode to display the level of logs sent to the log server.
--	---

→ Configuring the Facility Value of Logs Sent to the Log Server

Command	logging facility <i>facility-type</i>
Parameter Description	<i>facility-type</i> : Indicates the facility value of logs.
Command Mode	Global configuration mode
Configuration Usage	If the RFC5424 format is disabled, the facility value of logs sent to the server is local7 (23) by default. If the RFC5424 format is enabled, the facility value of logs sent to the server is local0 (16) by default.

→ Configuring the Source Interface of Logs Sent to the Log Server

Command	logging source [interface] <i>interface-type interface-number</i>
Parameter Description	<i>interface-type</i> : Indicates the interface type. <i>interface-number</i> : Indicates the interface number.
Command Mode	Global configuration mode
Configuration Usage	By default, the source interface of logs sent to the log server is the interface sending the logs. To facilitate management, you can use this command to set the source interface of all logs to an interface so that the administrator can identify the device that sends the logs based on the unique address.

→ Configuring the Source Address of Logs Sent to the Log Server

Command	logging source { ip ip-address ipv6 ipv6-address }
Parameter Description	ip ip-address : Specifies the source IPv4 address of logs sent to the IPv4 log server. ipv6 ipv6-address : Specifies the source IPv6 address of logs sent to the IPv6 log server.
Command Mode	Global configuration mode
Configuration Usage	By default, the source IP address of logs sent to the log server is the IP address of the interface sending the logs. To facilitate management, you can use this command to set the source IP address of all logs to the IP address of an interface so that the administrator can identify the device that sends the logs based on the unique address.

Configuration Example

→ Sending Syslogs to the Log Server

Scenario	It is required to configure the function of sending syslogs to the log server as follows: 1. Set the IPv4 address of the log server to 10.1.1.100. 2. Set the level of logs that can be sent to the log server to debugging (Level 7).
-----------------	--

	3. Set the source interface to Loopback 0.
Configuration Steps	<ul style="list-style-type: none">● Configure parameters for sending syslogs to the log server.
	<pre>QTECH# configure terminal QTECH(config)# logging server 10.1.1.100 QTECH(config)# logging trap debugging QTECH(config)# logging source interface Loopback 0</pre>
Verification	<ul style="list-style-type: none">● Run the show logging config command to display the configuration.
	<pre>QTECH#show logging config Syslog logging: enabled Console logging: level informational, 1307 messages logged Monitor logging: level informational, 0 messages logged Buffer logging: level informational, 1307 messages logged File logging: level informational, 122 messages logged File name:syslog_test.txt, size 128 Kbytes, have written 5 files Standard format:false Timestamp debug messages: datetime Timestamp log messages: datetime Sequence-number log messages: enable Sysname log messages: enable Count log messages: enable Trap logging: level debugging, 122 message lines logged,0 fail logging to 10.1.1.100</pre>

6.4.6. Writing Syslogs into Log Files

Configuration Effect

- Write syslogs into log files at the specified interval so that the administrator can view history logs anytime on the local device.

Notes

- Syslogs are not immediately written into log files. They are first buffered in the memory buffer, and then written into log files either periodically (at the interval of one hour by default) or when the buffer is full.

Configuration Steps

→ Writing Logs into Log Files

- (Mandatory) By default, syslogs are not written to any log file.
 - Unless otherwise specified, perform this configuration on every device.
- **Configuring the Interval at Which Logs Are Written into Log Files**
- (Optional) By default, syslogs are written to log files every hour.
 - Unless otherwise specified, perform this configuration on the device to configure the interval at which logs are written into log files.
- **Configuring the Storage Time of Log Files**
- (Optional) By default, no storage time is configured.
 - Unless otherwise specified, perform this configuration on the device to configure the storage time of log files.
- **Immediately Writing Logs in the Buffer into Log Files**
- (Optional) By default, syslogs are stored in the buffer and then written into log files periodically or when the buffer is full.
 - Unless otherwise specified, perform this configuration to write logs in the buffer into log files immediately. This command takes effect only once after it is configured.

Verification

- Run the **show logging config** command to display the configurations related to the log server.

Related Commands

→ Writing Logs into Log Files

Command	logging file { flash:filename usb0:filename usb1:filename } [max-file-size] [level]
Parameter Description	<p>flash: Indicates that log files will be stored on the extended Flash.</p> <p>usb0: Indicates that log files will be stored on USB 0. This option is supported only when the device has one USB port and a USB flash drive is inserted into the USB port.</p> <p>usb1: Indicates that log files will be stored on USB 1. This option is supported only when the device has two USB ports and USB flash drives are inserted into the USB ports.</p> <p>max-file-size: Indicates the maximum size of a log file. The value ranges from 128 KB to 6 MB. The default value is 128 KB.</p> <p>level: Indicates the level of logs that can be written into a log file.</p>
Command Mode	Global configuration mode
Configuration Usage	<p>This command is used to create a log file with the specified file name on the specified file storage device. The file size increases with the amount of logs, but cannot exceed the configured maximum size. If not specified, the maximum size of a log file is 128 KB by default.</p> <p>After this command is configured, the system saves logs to log files. A log file name does not contain any file name extension. The file name extension is always txt, which cannot be changed.</p> <p>After this command is configured, logs will be written into log files every hour. If you run the logging file flash:syslog command, a total of 16 log files will be created, namely, syslog.txt,</p>

syslog_1.txt, syslog_2.txt, ..., syslog_14.txt, and syslog_15.txt. Logs are written into the 16 log files in sequence. For example, the system writes logs into **syslog_1.txt** after **syslog.txt** is full. When **syslog_15.txt** is full, logs are written into **syslog.txt** again,


→ Configuring the Interval at Which Logs Are Written into Log Files

Command	logging flash interval <i>seconds</i>
Parameter Description	<i>seconds</i> : Indicates the interval at which logs are written into log files. The value ranges from 1s to 51,840s.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the interval at which logs are written into log files. The countdown starts after the command is configured.

→ Configuring the Storage Time of Log Files

Command	logging life-time level <i>level days</i>
Parameter Description	<i>level</i> : Indicates the log level. <i>days</i> : Indicates the storage time of log files. The unit is day. The storage time is not less than seven days.
Command Mode	Global configuration mode
Configuration Usage	After the log storage time is configured, the system writes logs of the same level that are generated in the same day into the same log file. The log file is named yyyy-mm-dd_filename_level.txt , where yyyy-mm-dd is the absolute time of the day when the logs are generated, filename is the log file named configured by the logging file flash command, and level is the log level. After you specify the storage time for logs of a certain level, the system deletes the logs after the storage time expires. Currently, the storage time ranges from 7days to 365 days. If the log storage time is not configured, logs are stored based on the file size to ensure compatibility with old configuration commands.

→ Immediately Writing Logs in the Buffer into Log Files

Command	logging flash flush
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	After this command is configured, syslogs are stored in the buffer and then written into log files periodically or when the buffer is full. You can run this command to immediately write logs into log files. <div style="border: 1px dashed black; padding: 5px;"> <p> The logging flash flush command takes effect once after it is configured. That is, after this command is configured, logs in the buffer are immediately written to log files.</p> </div>

Configuration Example

→ Writing Syslogs into Log Files

Scenario	It is required to configure the function of writing syslogs into log files as follows: 1. Set the log file name to syslog. 2. Set the level of logs sent to the Console to debugging (Level 7). 3. Set the interval at which device logs are written into files to 10 minutes (600s).
Configuration Steps	<ul style="list-style-type: none">● Configure parameters for writing syslogs into log files. <pre>QTECH# configure terminal QTECH(config)# logging file flash:syslog debugging QTECH(config)# logging flash interval 600</pre>
Verification	<ul style="list-style-type: none">● Run the show logging config command to display the configuration. <pre>QTECH(config)#show logging config Syslog logging: enabled Console logging: level informational, 1307 messages logged Monitor logging: level informational, 0 messages logged Buffer logging: level informational, 1307 messages logged File logging: level debugging, 122 messages logged File name:syslog.txt, size 128 Kbytes, have written 1 files Standard format:false Timestamp debug messages: datetime Timestamp log messages: datetime Sequence-number log messages: enable Sysname log messages: enable Count log messages: enable Trap logging: level debugging, 122 message lines logged,0 fail logging to 10.1.1.100</pre>

6.4.7. Configuring Syslog Filtering

Configuration Effect

- Filter out a specified type of syslogs if the administrator does not want to display these syslogs.
- By default, logs generated by all modules are displayed on the Console or other terminals. You can configure log filtering rules to display only desired logs.

Notes

- Two filtering modes are available: contains-only and filter-only. You can configure only one filtering mode at a time.
- If the same module, level, or mnemonic is configured in both the single-match and exact-match rules, the single-match rule prevails over the exact-match rule.

Configuration Steps

→ Configuring the Log Filtering Direction

- (Optional) By default, the filtering direction is all, that is, all logs are filtered out.
- Unless otherwise specified, perform this configuration on the device to configure the log filtering direction.

→ Configuring the Log Filtering Mode

- (Optional) By default, the log filtering mode is filter-only.
- Unless otherwise specified, perform this configuration on the device to configure the log filtering mode.

→ Configuring the Log Filtering Rule

- (Mandatory) By default, no filtering rule is configured.
- Unless otherwise specified, perform this configuration on the device to configure the log filtering rule.

Verification

- Run the **show running** command to display the configuration.

Related Commands

→ Configuring the Log Filtering Direction

Command	logging filter direction { all buffer file server terminal }
Parameter Description	all: Filters out all logs. buffer: Filters out logs sent to the log buffer, that is, the logs displayed by the show logging command. file: Filters out logs written into log files. server: Filters out logs sent to the log server. terminal: Filters out logs sent to the Console and VTY terminal (including Telnet and SSH).
Command Mode	Global configuration mode
Configuration Usage	The default filtering direction is all, that is, all logs are filtered out. Run the default logging filter direction command to restore the default filtering direction.

→ Configuring the Log Filtering Mode

Command	logging filter type { contains-only filter-only }
Parameter Description	contains-only: Indicates that only logs that contain keywords specified in the filtering rules are displayed.

	filter-only: Indicates that logs that contain keywords specified in the filtering rules are filtered out and will not be displayed.
Command Mode	Global configuration mode
Configuration Usage	Log filtering modes include contains-only and filter-only. The default filtering mode is filter-only.

→ Configuring the Log Filtering Rule

Command	logging filter rule { exact-match module <i>module-name</i> mnemonic <i>mnemonic-name</i> level <i>level</i> single-match { level <i>level</i> mnemonic <i>mnemonic-name</i> module <i>module-name</i> } }
Parameter Description	exact-match: If exact-match is selected, you must specify all three filtering options. single-match: If single-match is selected, you may specify only one of the three filtering options. module <i>module-name</i> : Indicates the module name. Logs of this module will be filtered out. mnemonic <i>mnemonic-name</i> : Indicates the mnemonic. Logs with this mnemonic will be filtered out. level <i>level</i> : Indicates the log level. Logs of this level will be filtered out.
Command Mode	Global configuration mode
Configuration Usage	Log filtering rules include exact-match and single-match. The no logging filter rule exact-match [module <i>module-name</i> mnemonic <i>mnemonic-name</i> level <i>level</i>] command is used to delete the exact-match filtering rules. You can delete all exact-match filtering rules at a time or one by one. The no logging filter rule single-match [level <i>level</i> mnemonic <i>mnemonic-name</i> module <i>module-name</i>] command is used to delete the single-match filtering rules. You can delete all single-match filtering rules at a time or one by one.

Configuration Example

→ Configuring Syslog Filtering

Scenario	It is required to configure the syslog filtering function as follows: 1. Set the filtering directions of logs to terminal and server . 2. Set the log filtering mode to filter-only. 3. Set the log filtering rule to single-match to filter out logs that contain the module name "SYS".
Configuration Steps	<ul style="list-style-type: none"> ● Configure the syslog filtering function.
	<pre>QTECH# configure terminal QTECH(config)# logging filter direction server QTECH(config)# logging filter direction terminal QTECH(config)# logging filter type filter-only QTECH(config)# logging filter rule single-match module SYS</pre>
Verification	<ul style="list-style-type: none"> ● Run the show running-config include logging command to display the configuration.

	<ul style="list-style-type: none">• Enter and exit global configuration mode, and verify that the system displays logs accordingly.
	<pre>QTECH#configure Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)#exit QTECH# QTECH#show running-config include logging logging filter direction server logging filter direction terminal logging filter rule single-match module SYS</pre>

6.4.8. Configuring Syslog Redirection

Configuration Effect

- On the VSU, logs on the secondary or standby device are displayed on its Console window, and redirected to the active device for display on the Console or VTY window, or stored in the memory buffer, extended flash, or syslog server.
- On a box-type VSU, after the log redirection function is enabled, logs on the secondary or standby device will be redirected to the active device, and the role flag (*device ID) will be added to each log to indicate that the log is redirected. Assume that four devices form a VSU. The ID of the active device is 1, the ID of the secondary device is 2, and the IDs of two standby devices are 3 and 4. The role flag is not added to logs generated by the active device. The role flag (*2) is added to logs redirected from the secondary device to the active device. The role flags (*3) and (*4) are added respectively to logs redirected from the two standby devices to the active device.
- On a card-type VSU, after the log redirection function is enabled, logs on the secondary or standby supervisor module will be redirected to the active supervisor module, and the role flag "(device ID/supervisor module name)" will be added to each log to indicate that the log is redirected. If four supervisor modules form a VSU, the role flags are listed as follows: (*1/M1), (*1/M2), (*2/M1), and (*2/M2).

Notes

- The syslog redirection function takes effect only on the VSU.
- You can limit the rate of logs redirected to the active device to prevent generating a large amount of logs on the secondary or standby device.

Configuration Steps

→ Enabling Log Redirection

- (Optional) By default, log redirection is enabled on the VSU.
- Unless otherwise specified, perform this configuration on the active device of VSU or active supervisor module.

→ Configuring the Rate Limit

- (Optional) By default, a maximum of 200 logs can be redirected from the standby device to the active device of VSU per second.
- Unless otherwise specified, perform this configuration on the active device of VSU or active supervisor module.

Verification

- Run the **show running** command to display the configuration.

Related Commands

→ Enabling Log Redirection

Command	logging rd on
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	By default, log redirection is enabled on the VSU.

→ Configuring the Rate Limit

Command	logging rd rate-limit <i>number</i> [except <i>level</i>]
Parameter Description	rate-limit <i>number</i> : Indicates the maximum number of logs redirected per second. The value ranges from 1 to 10,000. except <i>level</i> : Rate limit is not applied to logs with a level equaling to or lower than the specified severity level. By default, the severity level is error (Level 3), that is, rate limit is not applied to logs of Level 3 or lower.
Command Mode	Global configuration mode
Configuration Usage	By default, a maximum of 200 logs can be redirected from the standby device to the active device of VSU per second.

Configuration Example

→ Configuring Syslog Redirection

Scenario	It is required to configure the syslog redirection function on the VSU as follows: 1. Enable the log redirection function. 2. Set the maximum number of logs with a level higher than critical (Level 2) that can be redirected per second to 100.
-----------------	--

Configuration Steps	<ul style="list-style-type: none">● Configure the syslog redirection function.
	<pre>QTECH# configure terminal QTECH(config)# logging rd on QTECH(config)# logging rd rate-limit 100 except critical</pre>
Verification	<ul style="list-style-type: none">● Run the show running-config include logging command to display the configuration.● Generate a log on the standby device, and verify that the log is redirected to and displayed on the active device.
	<pre>QTECH#show running-config include logging logging rd rate-limit 100 except critical</pre>

6.4.9. Configuring Syslog Monitoring

Configuration Effect

- Record login/exit attempts. After logging of login/exit attempts is enabled, the related logs are displayed on the device when users access the device through Telnet or SSH. This helps the administrator monitor the device connections.
- Record modification of device configurations. After logging of operations is enabled, the related logs are displayed on the device when users modify the device configurations. This helps the administrator monitor the changes in device configurations.

Notes

- If both the **logging userinfo** command and the **logging userinfo command-log** command are configured on the device, only the configuration result of the **logging userinfo command-log** command is displayed when you run the **show running-config** command.

Configuration Steps

→ Enabling Logging of Login/Exit Attempts

- (Optional) By default, logging of login/exit attempts is disabled.
- Unless otherwise specified, perform this configuration on every line of the device to enable logging of login/exit attempts.

→ Enabling logging of Operations

- (Optional) By default, logging of operations is disabled.
- Unless otherwise specified, perform this configuration on every line of the device to enable logging of operations.

Verification

- Run the **show running** command to display the configuration.

Related Commands

→ Enabling Logging of Login/Exit Attempts

Command	logging userinfo
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	By default, a device does not generate related logs when users log into or exit the device.

→ Enabling Logging of Operations

Command	logging userinfo command-log
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	The system generates related logs when users run configuration commands. By default, a device does not generate logs when users modify device configurations.

Configuration Example

→ Configuring Syslog Monitoring

Scenario	It is required to configure the syslog monitoring function as follows: 1. Enable logging of login/exit attempts. 2. Enable logging of operations.
Configuration Steps	<ul style="list-style-type: none"> • Configure the syslog monitoring function.
	<pre>QTECH# configure terminal QTECH(config)# logging userinfo QTECH(config)# logging userinfo command-log</pre>
Verification	<ul style="list-style-type: none"> • Run the <code>show running-config include logging</code> command to display the configuration. • Run a command in global configuration mode, and verify that the system generates a log.
	<pre>QTECH#configure terminal</pre>


```
Enter configuration commands, one per line. End with CNTL/Z.  
QTECH(config)#interface gigabitEthernet 0/0  
*Jun 16 15:03:43: %CLI-5-EXEC_CMD: Configured from console by admin  
command: interface GigabitEthernet 0/0  
QTECH#show running-config | include logging  
logging userinfo command-log
```

6.4.10. Synchronizing User Input with Log Output

Configuration Effect

- By default, the user input is not synchronized with the log output. After this function is enabled, the content input during log output is displayed after log output is completed, ensuring integrity and continuity of the input.

Notes

- This command is executed in line configuration mode. You need to configure this command on every line as required.

Configuration Steps

→ Synchronizing User Input with Log Output

- (Optional) By default, the synchronization function is disabled.
- Unless otherwise specified, perform this configuration on every line to synchronize user input with log output.

Verification

- Run the **show running** command to display the configuration.

Related Commands

→ Synchronizing User Input with Log Output

Command	logging synchronous
Parameter Description	N/A
Command Mode	Line configuration mode
Configuration Usage	This command is used to synchronize the user input with log output to prevent interrupting the user input.

Configuration Example

→ Synchronizing User Input with Log Output

Scenario	It is required to synchronize the user input with log output as follows:
-----------------	--

	1. Enable the synchronization function.
Configuration Steps	<ul style="list-style-type: none"> Configure the synchronization function.
	<pre>QTECH# configure terminal QTECH(config)# line console 0 QTECH(config-line)# logging synchronous</pre>
Verification	<ul style="list-style-type: none"> Run the show running-config begin line command to display the configuration.
	<pre>QTECH#show running-config begin line line con 0 logging synchronous login local</pre> <p>As shown in the following output, when a user types in "vlan", the state of interface 0/1 changes and the related log is output. After log output is completed, the log module automatically displays the user input "vlan" so that the user can continue typing.</p> <pre>QTECH(config)#vlan *Aug 20 10:05:19: %LINK-5-CHANGED: Interface GigabitEthernet 0/1, changed state to up *Aug 20 10:05:19: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/1, changed state to up QTECH(config)#vlan</pre>

6.5. Monitoring

Clearing

 Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears logs in the memory buffer.	clear logging

Displaying

Description	Command
Displays log statistics and logs in the memory buffer based on the timestamp from oldest to latest.	show logging
Displays syslog configurations and statistics.	show logging config
Displays log statistics of each module in the system.	show logging count

7. CONFIGURING CWMP

7.1. Overview

CPE WAN Management Protocol (CWMP) provides a general framework of unified device management, related message specifications, management methods, and data models, so as to solve difficulties in unified management and maintenance of dispersed customer-premises equipment (CPEs), improve troubleshooting efficiency, and save O&M costs.

CWMP provides the following functions:

- **Auto configuration and dynamic service provisioning.** CWMP allows an Auto-Configuration Server (ACS) to automatically provision CPEs who initially access the network after start. The ACS can also dynamically re-configure running CPEs.
- **Firmware management.** CWMP manages and upgrades the firmware and its files of CPEs.
- **Software module management.** CWMP manages modular software according to data models implemented.
- **Status and performance monitoring.** CWMP enables CPEs to notify the ACE of its status and changes, achieving real-time status and performance monitoring.
- **Diagnostics.** The ACE diagnoses or resolves connectivity or service problems based on information from CPEs, and can also perform defined diagnosis tests.

Protocols and Standards

For details about TR069 protocol specifications, visit <http://www.broadband-forum.org/technical/trlist.php>.

Listed below are some major CWMP protocol specifications:

- TR-069_Amendment-4.pdf: CWMP standard
- TR-098_Amendment-2.pdf: Standard for Internet gateway device data model
- TR-106_Amendment-6.pdf: Standard for CPE data model
- TR-181_Issue-2_Amendment-5.pdf: Standard for CPE data model 2
- tr-098-1-4-full.xml: Definition of Internet gateway device data model
- tr-181-2-4-full.xml: Definition 2 of CPE data model 2

7.2. Applications

Typical Application	Scenario
---------------------	----------

**CWMP Network
Application Scenario**

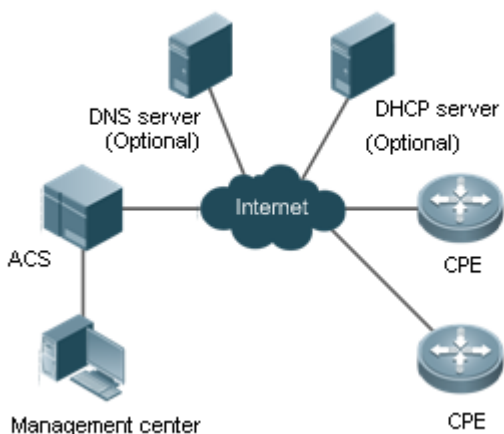
Initiate CPE-ACS connection, so as to upgrade the CPE firmware, upload the configuration files, restore the configuration, and realize other features.

7.2.1. CWMP Network Application Scenario

Application Scenario

The major components of a CWMP network architecture are CPEs, an ACS, a management center, a DHCP server, and a Domain Name System (DNS) server. The management center manages a population of CPEs by controlling the ACS on a Web browser.

Figure 7-1



Note

- If the Uniform Resource Locator (URL) of the ACS is configured on CPEs, the DHCP server is optional. If not, the DHCP is required to dynamically discover the ACS URL.
- If the URLs of the ACS and CPEs contain IP addresses only, the DNS server is optional. If their URLs contain domain names, the DNS server is required to resolve the names.

Functional Deployment

HTTP runs on both CPEs and the ACS.

7.3. Features

Basic Concept

→ Major Terminologies

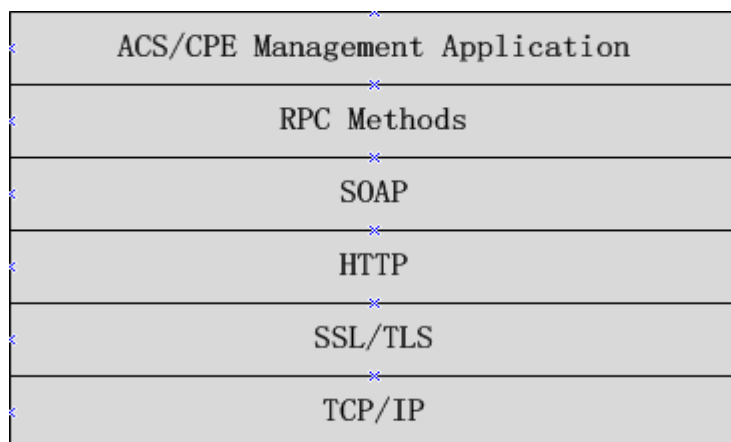
- **CPE:** Customer Premises Equipment
- **ACS:** Auto-Configuration Server

- **RPC:** Remote Procedure Call
- **DM:** Data Model

➔ **Protocol Stack**

Figure 7-2 shows the protocol stack of CWMP.

Figure 7-2 CWMP Protocol Stack



As shown in Figure 7-2, CWMP defines six layers with respective functions as follows:

- **ACS/CPE Application**

The application layer is not a part of CWMP. It is the development performed by various modules of the CPEs/ACS to support CWMP, just like the Simple Network Management Protocol (SNMP), which does not cover the MIB management of functional modules.

- **RPC Methods**

This layer provides various RPC methods for interactions between the ACS and the CPEs.

- **SOAP**

The Simple Object Access Protocol (SOAP) layer uses a XML-based syntax to encode and decode CWMP messages. Thus, CWMP messages must comply with the XML-based syntax.

- **HTTP**

All CWMP messages are transmitted over Hypertext Transfer Protocol (HTTP). Both the ACS and the CPEs can behave in the role of HTTP clients and servers. The server function is used to monitor reverse connections from the peer.

- **SSL/TLS**

The Secure Sockets Layer (SSL) or Transport Layer Security (TLS) layer guarantees CWMP security, including data integrity, confidentiality, and authentication.

- **TCP/IP**

This layer is the (Transmission Control Protocol/Internet Protocol (TCP/IP) protocol stack.

→ RPC Methods

The ACS manages and monitors CPEs by calling mostly the following RPC methods:

- **Get RPC Methods**

The Get methods enable the ACS to remotely obtain the set of RPC methods, as well as names, values and attributes of the DM parameters supported on CPEs.

- **Set RPC Methods**

The Set methods enable the ACS to remotely set the values and attributes of the DM parameters supported on CPEs.

- **Inform RPC Methods**

The Inform methods enable CPEs to inform the ACS of their device identifiers, parameter information, and events whenever sessions are established between them.

- **Download RPC Methods**

The Download method enables the ACS to remotely control the file download of CPEs, including firmware management, upgrade, and Web package upgrade.

- **Upload RPC Methods**

The Upload method enables the ACS to remotely control the file upload of CPEs, including upload of firmware and logs.

- **Reboot RPC Methods**

The Reboot method enables the ACS to remotely reboot the CPEs.

→ Session Management

CWMP sessions or interactions are the basis for CWMP. All CWMP interactions between the ACS and CPEs rely on their sessions. CWMP helps initiate and maintain ACS-CPE sessions to link them up for effective management and monitoring. An ACS-CPE session is a TCP connection, which starts from the Inform negotiation to TCP disconnection. The session is classified into CPE Initiated Session and ACS Initiated Session according to the session poster.

→ DM Management

CWMP operates based on CWMP Data Model (DM). CWMP manages all functional modules by a set of operations performed on DM. Each functional module registers and implements a respective data model, just like the MIBs implemented by various functional modules of SNMP.

A CWMP data model is represented in the form of a character string. For a clear hierarchy of the data model, a dot (.) is used as a delimiter to distinguish an upper-level data model node from a lower-level data model node. For instance, in the data model

InternetGatewayDevice.LANDevice, InternetGatewayDevice is the parent data model node of **LANDevice**, and **LANDevice** is the child data model node of **InternetGatewayDevice**.

DM nodes are classified into two types: object nodes and parameter nodes. The parameter nodes are also known as leaf nodes. An object node is a node under which there are child nodes, and a parameter node is a leaf node under which there is no any child node. Object nodes are further classified into single-instance object nodes and multi-instance object nodes. A single-instance object node is an object node for which there is only one instance, whereas a multi-instance object node is an object node for which there are multiple instances.

DM nodes can also be classified into readable nodes and readable-and-writable nodes. A readable node is a node whose parameter values can be read but cannot be modified, and a readable-and-writable node is a node whose parameter values can be both read and modified.

A data model node has two attributes. One attribute relates to a notification function; that is, whether to inform the ACS of changes (other than changes caused by CWMP) to parameter values of the data model. The other attribute is an identifier indicating that the parameters of the data model node can be written using other management modes (than the ACS); that is, whether the values of the parameters can be modified using other management modes such as Telnet. The ACS can modify the attributes of the data models using RPC methods.

CWMP manages the data models using corresponding RPC methods.

→ Event Management

When some events concerned by the ACS occur on the CPE, the CPE will inform the ACS of these events. The ACS monitors these events to monitor the working status of the CPE. The CWMP events are just like Trap messages of SNMP or product logs. Using RPC methods, to the ACS filters out the unconcerned types of events. CWMP events are classified into two types: single or (not cumulative) events and multiple (cumulative) events. A single event means that there is no quantitative change to the same event upon re-occurrence of the event, with the old discarded and the newest kept. A multiple event means that the old are not discarded and the newest event is kept as a complete event when an event re-occurs for multiple times later; that is, the number of this event is incremented by 1.

All events that occur on the CPE are notified to the ACS using the INFORM method.

Features

Feature	Description
Upgrading the Firmware	The ACS controls the upgrade of the firmware of a CPE using the Download method.

<u>Upgrading the Configuration Files</u>	The ACS controls the upgrade of the configuration files of a CPE using the Download method.
<u>Uploading the Configuration Files</u>	The ACS controls the upload of the configuration files of a CPE using the Upload method.
<u>Backing up and Restoring a CPE</u>	When a CPE breaks away from the management center, this feature can remotely restore the CPE to the previous status.

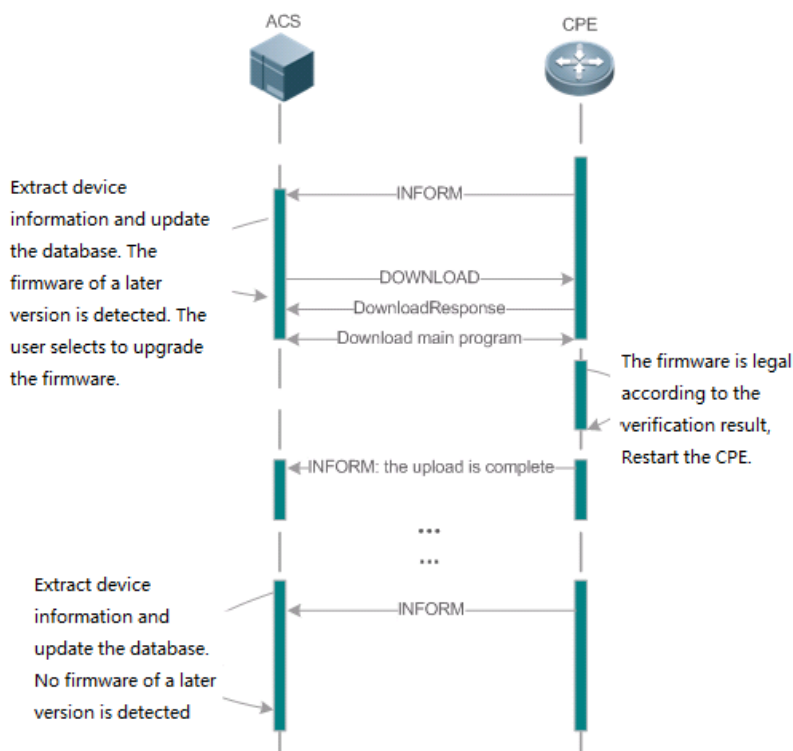
7.3.1. Upgrading the Firmware

Upgrading the Firmware means the firmware of a network element (NE) can be upgraded, so as to implement device version upgrade or replacement.

Working Principle

→ Sequence Diagram of Upgrading the Firmware

Figure 7-3



Users specify a CPE for the ACS to deliver the Download method for upgrading the firmware. The CPE receives the request and starts to download the latest firmware from the destination file server, upgrade the firmware, and then reboot. After restart, the CPE will indicate the successful or unsuccessful completion of the method application.

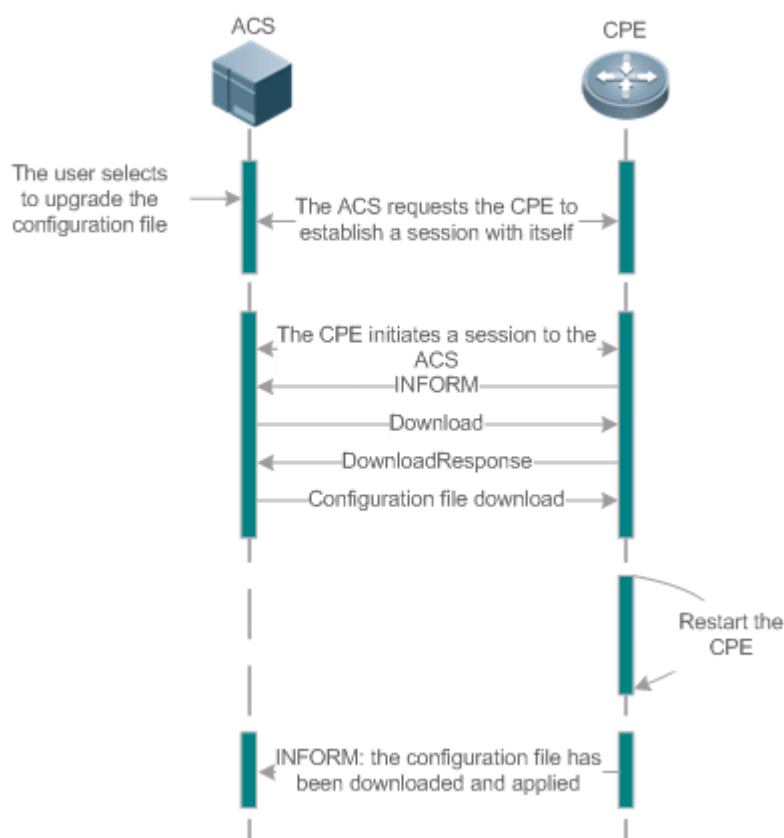
🔗 The file server can be ACS or separately deployed.

7.3.2. Upgrading the Configuration Files

Upgrading the Configuration Files means the current configuration files of a CPE can be replaced with specified configuration files, so that the new configuration files act on the CPE after reset.

Working Principle

Figure 7-4



Users specify a CPE for the ACS to deliver the Download methods for upgrading its configuration files. The CPE downloads the configuration files from the specified file server, upgrade configuration files, and then reboot. After that, the CPE will indicate successful or unsuccessful completion of the method application.

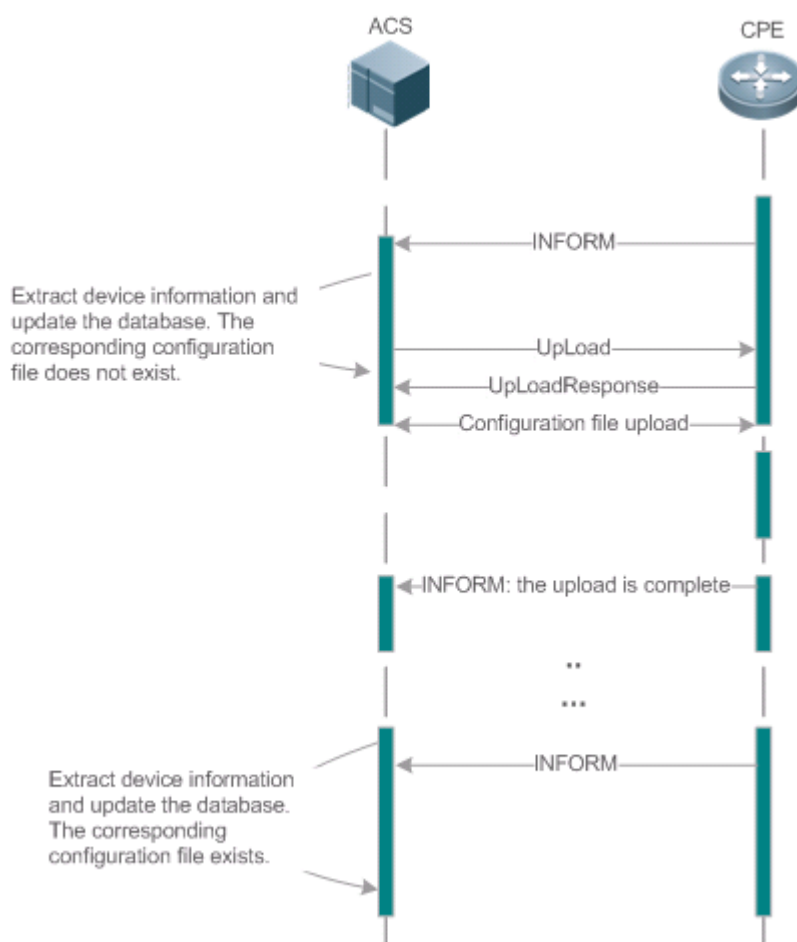
↳ The file server can be ACS or separately deployed.

7.3.3. Uploading the Configuration Files

Uploading the Configuration Files means the ACS controls the configuration files of CPEs by using the Upload method.

Working Principle

Figure 7-5



When a CPE initially accesses the ACS, the ACS attempts to learn the configuration files of the CPE in the following sequence:

- When the ACS initially receives an Inform message from the CPE, it locates the corresponding database information according to device information carried in the message.

- If the database does not contain the configuration files of the CPE, the ACS delivers the Upload method to the CPE for uploading the configuration files.
- The CPE uploads its current configuration files to the ACS.
- The CPE returns a successful or unsuccessful response to the Upload request.

7.3.4. Backing Up and Restoring a CPE


When a remote CPE breaks away from the management center due to abnormal operations, the CPE backup and restoration feature helps restore the CPE to the previous status, so that the management center can resume the supervision of the CPE as necessary.



Working Principle

You can configure the restoration function on a CPE, so that the CPE can restore itself from exceptions of its firmware or configuration files. Then when the CPE fails to connect to the ACS and breaks away from the management center after its firmware or configuration files are upgraded, the previous firmware or configuration files of the CPE can be restored in time for the ACS to manage the CPE. This kind of exception is generally caused by delivery of a wrong version or configuration file.

Before the CPE receives a new firmware or configuration files to upgrade, the CPE will back up its current version and configuration files. In addition, there is a mechanism for determining whether the problem described in the preceding scenario has occurred. If the problem has occurred, the CPE is restored to the previous manageable status.

7.4. Configuration

Action	Suggestions and Related Commands	
Establishing a Basic CWMP Connection	 (Mandatory) You can configure the ACS or CPE usernames and passwords to be authenticated for CWMP connection.	
	cwmp	Enables CWMP and enters CWMP configuration mode.
	acs username	Configures the ACS username for CWMP connection.
	acs password	Configures the ACS password for CWMP connection.
	cpe username	Configures the CPE username for CWMP connection.
	cpe password	Configures the CPE password for CWMP connection.

	<p> (Optional) You can configure the URLs of the CPE and the ACS.</p>	
	acs url	Configures the ACS URL.
	cpe url	Configures the CPE URL.
<u>Configuring CWMP-Related Attributes</u>	<p> (Optional) You can configure the basic functions of the CPE, such as upload, backup and restoration of firmware, configuration files or logs.</p>	
	cpe inform	Configures the periodic notification function of the CPE.
	cpe back-up	Configures the backup and restoration of the firmware and configuration file of the CPE.
	disable download	Disables the function of downloading firmware and configuration files from the ACS.
	disable upload	Disables the function of uploading configuration and log files to the ACS.
	timer cpe- timeout	Configures the ACS response timeout on CPEs.

7.4.1. Establishing a Basic CWMP Connection

Configuration Effect

- A session connection is established between the ACS and the CPE.

Precautions

- N/A

Configuration Method

→ Enabling CWMP and Entering CWMP Configuration Mode

- (Mandatory) The CWMP function is enabled by default.

Command	cwmp
Parameter Description	N/A
Defaults	CWMP is enabled by default.
Command Mode	Global configuration guide

Usage Guide	N/A
--------------------	-----

→ **Configuring the ACS Username for CWMP Connection**

- This configuration is mandatory on the ACS.
- Only one username can be configured for the ACS. If multiple are configured, the latest configuration is applied.

Command	acs username <i>username</i>
Parameter Description	username <i>username</i> : The ACS username for CWMP connection
Defaults	The ACS username is not configured by default.
Command Mode	CWMP configuration mode
Usage Guide	N/A

→ **Configuring the ACS Password for CWMP Connection**

- This configuration is mandatory on the ACS.
- The password of the ACS can be in plaintext or encrypted form. Only one password can be configured for the ACS. If multiple are configured, the latest configuration is applied.

Command	acs password { <i>password</i> <i>encryption-type encrypted-password</i> }
Parameter Description	<i>password</i> : ACS password <i>encryption-type</i> : 0 (no encryption) or 7 (simple encryption) <i>encrypted-password</i> : Password text
Defaults	<i>encryption-type</i> : 0 <i>encrypted-password</i> : N/A
Command Mode	CWMP configuration mode
Usage Guide	N/A

→ **Configuring the CPE Username for CWMP Connection**

- This configuration is mandatory on the CPE.
- Only one username can be configured for the CPE. If multiple are configured, the latest configuration is applied.

Command	cpe username <i>username</i>
Parameter Description	<i>username</i> : CPE username

Defaults	No CPE username is configured by default.
Command Mode	CWMP configuration mode
Usage Guide	N/A

→ Configuring the CPE Password for CWMP Connection

- This configuration is mandatory on the CPE.
- The password of the CPE can be in plaintext or encrypted form. Only one password can be configured for the CPE. If multiple are configured, the latest configuration is applied.

Command	cpe password { <i>password</i> <i>encryption-type</i> <i>encrypted-password</i> }
Parameter Description	<i>password</i> : CPE password <i>encryption-type</i> : 0 (no encryption) or 7 (simple encryption) <i>encrypted-password</i> : Password text
Defaults	<i>encryption-type</i> : 0 <i>encrypted-password</i> : N/A
Command Mode	CWMP configuration mode
Usage Guide	Use this command to configure the CPE user password to be authenticated for the ACS to connect to the CPE. In general, the encryption type does not need to be specified. The encryption type needs to be specified only when copying and pasting the encrypted password of this command. A valid password should meet the following format requirements: <ul style="list-style-type: none"> • Contain 1 to 26 characters including letters and figures. • The leading spaces will be ignored, while the trailing and middle are valid. • If 7 (simple encryption) is specified, the valid characters only include 0 to 9 and a (A) to f (F).

→ Configuring the ACS URL for CMWP Connection

- This configuration is optional on the CPE.
- Only one ACS URL can be configured. If multiple are configured, the latest configuration is applied. The ACS URL must be in HTTP format.

Command	acs url <i>url</i>
Parameter Description	<i>url</i> : ACS URL
Defaults	No ACS URL is configured by default.
Command Mode	CWMP configuration mode

Usage Guide	<p>If the ACS URL is not configured but obtained through DHCP, CPEs will use this dynamic URL to initiate connection to the ACS. The ACS URL must:</p> <ul style="list-style-type: none"> ● Be in format of http://host[:port]/path or https://host[:port]/path. ● Contain 256 characters at most.
--------------------	--

→ **Configuring the CPE URL for CWMP Connection**

- This configuration is optional on the CPE.
- Only one CPE URL can be configured. If multiple are configured, the latest configuration is applied. The CPE URL must be in HTTP format instead of domain name format.

Command	cpe url url
Parameter Description	url: CPE URL
Defaults	No CPE URL is configured by default.
Command Mode	CWMP configuration mode
Usage Guide	<p>If CPE URL is not configured, it is obtained through DHCP. The CPE URL must:</p> <ul style="list-style-type: none"> ● Be in format of http://ip [: port]/. ● Contain 256 characters at most.

Verification

- Run the **show cwmp configuration** command.


Command	show cwmp configuration
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A
Configuration Examples	<p>The following example displays the CWMP configuration.</p> <pre> QTECH(config-cwmp)#show cwmp configuration CWMP Status : enable ACS URL : http://www.qtech.ru/acs ACS username : admin ACS password : ***** CPE URL : http://10.10.10.2:7547/ CPE username : qtech CPE password : ***** </pre>

```
CPE inform status           : disable
CPE inform interval        : 60s
CPE inform start time      : 0:0:0 0 0 0
CPE wait timeout           : 50s
CPE download status        : enable
CPE upload status          : enable
CPE back up status         : enable
CPE back up delay time     : 60s
```

Configuration Examples

↪ The following configuration examples describe CWMP-related configuration only.

→ Configuring Usernames and Passwords on the CPE

<p>Network Environment Figure 7-6</p>	
<p>Configuration Method</p>	<ul style="list-style-type: none"> • Enable CWMP. • On the CPE, configure the ACS username and password to be authenticated for the CPE to connect to the ACS. • On the CPE, configure the CPE username and password to be authenticated for the ACS to connect to the CPE.
<p>CPE</p>	<pre>QTECH# configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)# cwmp QTECH(config-cwmp)# acs username USERB QTECH(config-cwmp)# acs password PASSWORDB QTECH(config-cwmp)# cpe username USERB QTECH(config-cwmp)# cpe password PASSWORDB</pre>
<p>Verification</p>	<ul style="list-style-type: none"> • Run the show command on the CPE to check whether the configuration commands have been successfully applied.
<p>CPE</p>	<pre>QTECH # show cwmp configuration CWMP Status : enable ACS URL : http://10.10.10.1:7547/acs ACS username : USERA ACS password : *****</pre>

```
CPE URL : http://10.10.10.2:7547/
CPE username : USERB
CPE password : *****
```

→ Configuring the URLs of the ACS and the CPE

Network Environment	See Figure 7-6.
Configuration Method	<ul style="list-style-type: none"> ● Configure the ACS URL. ● Configure the CPE URL.
CPE	<pre>QTECH# configure terminal QTECH(config)# cwmp QTECH(config-cwmp)# acs url http://10.10.10.1:7547/acs QTECH(config-cwmp)# cpe url http://10.10.10.1:7547/</pre>
Verification	Run the show command on the CPE to check whether the configuration commands have been successfully applied.
CPE	<pre>QTECH #show cwmp configuration CWMP Status : enable ACS URL : http://10.10.10.1:7547/acs ACS username : USERA ACS password : ***** CPE URL : http://10.10.10.2:7547/</pre>

Common Errors

- The user-input encrypted password is longer than 254 characters, or the length of the password is not an even number.
- The user-input plaintext password is longer than 100 characters.
- The user-input plaintext password contains illegal characters.
- The user-input encrypted password contains illegal characters (the legitimate characters includes only 0~9, a~f and A~F)
- The URL of the ACS is set to NULL.
- The URL of the CPE is set to NULL.

7.4.2. Configuring CWMP-Related Attributes

Configuration Effect

- You can configure common functions of the CPE, such as the backup and restoration of its firmware or configuration file, whether to enable the CPE to download firmware and

configuration files from the ACS, and whether to enable the CPE to upload its configuration and log files to the ACS.

Configuration Method

→ Configuring the Periodic Notification Function of the CPE

- (Optional) The value range is from 30 to 3,600 in seconds. The default value is 600 seconds.
- Perform this configuration to reset the periodical notification interval of the CPE.

Command	cpe inform [interval seconds] [starttime time]
Parameter Description	<i>seconds</i> : Specifies the periodical notification interval of the CPE. The value range is from 30 to 3,600 in seconds. <i>time</i> : Specifies the date and time for starting periodical notification in yyyy-mm-ddThh:mm:ss format.
Command Mode	CWMP configuration mode
Defaults	The default value is 600 seconds.
Usage Guide	Use this command to configure the periodic notification function of the CPE. <ul style="list-style-type: none"> • If the time for starting periodical notification is not specified, periodical notification starts after the periodical notification function is enabled. The notification is performed once within every notification interval. • If the time for starting periodical notification is specified, periodical notification starts at the specified start time. For instance, if the periodical notification interval is set to 60 seconds and the start time is 12:00 am next day, periodical notification will start at 12:00 am next day and once every 60 seconds.

→ Disabling the Function of Downloading Firmware and Configuration Files from the ACS

- (Optional) The CPE can download firmware and configuration files from the ACS by default.
- Perform this configuration if the CPE does not need to download firmware and configuration files from the ACS.

Command	disable download
Parameter Description	N/A
Defaults	The CPE can download firmware and configuration files from the ACS by default.
Command Mode	CWMP configuration mode

Usage Guide	Use this command to disable the function of downloading main program and configuration files from the ACS. <ul style="list-style-type: none"> • This command does not act on configuration script files. The configuration scripts can still be executed even if this function is disabled.
--------------------	--

→ **Disabling the Function of Uploading Configuration and Log Files to the ACS**

- (Optional.) The CPE can upload configuration and log files to the ACS by default.
- Perform this configuration if the CPE does not need to upload configuration and log files to the ACS.

Command	disable upload
Parameter Description	N/A
Defaults	The CPE can upload configuration and log files to the ACS by default.
Command Mode	CWMP configuration mode
Usage Guide	Use this command to disable the function of uploading configuration and log files to the ACS.

→ **Configuring the Backup and Restoration of the Firmware and Configuration Files of the CPE**

- (Optional) The backup and restoration of the firmware and configuration files of the CPE is enabled by default. The value range is from 30 to 10,000 in seconds. The default value is 60 seconds.
- The longer the delay-time is, the longer the reboot will be complete.
- Perform this configuration to modify the function of backing up and restoring the firmware and configuration files of the CPE.

Command	cpe back-up [delay-time seconds]
Parameter Description	<i>seconds</i> : Specifies the delay for backup and restoration of the firmware and configuration file of the CPE.
Defaults	The default value is 60 seconds.
Command Mode	CWMP configuration mode
Usage Guide	N/A

→ **Configuring the ACS Response Timeout**

- (Optional) The value range is from 10 to 600 in seconds. The default value is 30 seconds.
- Perform this configuration to modify the ACS response timeout period on the CPE.

Command	timer cpe- timeout seconds
Parameter Description	<i>seconds</i> : Specifies the timeout period in seconds. The value range is from 10 to 600.
Defaults	The default value is 30 seconds.
Command Mode	CWMP configuration mode
Usage Guide	N/A

Verification

- Run the **show cwmp configuration** command.

Command	show cwmp configuration
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A
Configuration Examples	<p>The following example displays the CWMP configuration.</p> <pre> QTECH(config-cwmp)#show cwmp configuration CWMP Status : enable ACS URL : http://www.qtech.ru/acs ACS username : admin ACS password : ***** CPE URL : http://10.10.10.2:7547/ CPE username : qtech CPE password : ***** CPE inform status : disable CPE inform interval : 60s CPE inform start time : 0:0:0 0 0 0 CPE wait timeout : 50s CPE download status : enable CPE upload status : enable CPE back up status : enable CPE back up delay time : 60s </pre>

Configuration Examples

→ Configuring the Periodical Notification Interval of the CPE

Network Environment	See Figure 7-6.
Configuration Steps	<ul style="list-style-type: none"> ● Enable the CWMP function and enter CWMP configuration mode. ● Set the periodical notification interval of the CPE to 60 seconds.
CPE	<pre>QTECH#config Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)#cwmp QTECH(config-cwmp)#cpe inform interval 60</pre>
Verification	Run the show command on the CPE to check whether the configuration commands have been successfully applied.
CPE	<pre>QTECH #show cwmp configuration CWMP Status : enable CPE inform interval : 60s</pre>

→ Disabling the Function of Downloading Firmware and Configuration Files from the ACS

Network Environment	See Figure 7-6.
Steps	<ul style="list-style-type: none"> ● Enable the CWMP function and enter CWMP configuration mode. ● Disable the function of downloading firmware and configuration files from the ACS.
CPE	<pre>QTECH#config Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)#cwmp QTECH(config-cwmp)#disable download</pre>
Verification	Run the show command on the CPE to check whether the configuration commands have been successfully applied.
CPE	<pre>QTECH #show cwmp configuration CWMP Status : enable CPE download status : disable</pre>

→ Disabling the Function of Uploading Configuration and Log Files to the ACS

Network Environment	See Figure 7-6.
----------------------------	-----------------

Configuration Steps	<ul style="list-style-type: none"> ● Enable the CWMP function and enter CWMP configuration mode. ● Disable the CPE's function of uploading configuration and log files to the ACS.
CPE	<pre>QTECH#config Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)#cwmp QTECH(config-cwmp)# disable upload</pre>
Verification	Run the show command on the CPE to check whether the configuration commands have been successfully applied.
CPE	<pre>QTECH #show cwmp configuration CWMP Status : enable CPE upload status : disable</pre>

→ Configuring the Backup and Restoration Delay

Network Environment	See Figure 7-6.
Configuration Steps	<ul style="list-style-type: none"> ● Enable the CWMP function and enter CWMP configuration mode. ● Set the backup and restoration delay to 100 seconds.
CPE	<pre>QTECH#config Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)#cwmp QTECH(config-cwmp)# cpe back-up Seconds 30</pre>
Verification	Run the show command on the CPE to check whether the configuration commands have been successfully applied.
CPE	<pre>QTECH #show cwmp configuration CWMP Status : enable CPE back up delay time : 30s</pre>

→ Configuring the ACS Response Timeout of the CPE

Network Environment	See Figure 7-6.
Configuration Steps	<ul style="list-style-type: none"> ● Enable the CWMP function and enter CWMP configuration mode.

	<ul style="list-style-type: none"> ● Set the response timeout of the CPE to 100 seconds.
CPE	<pre>QTECH# configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)# cwmp QTECH(config-cwmp)# timer cpe-timeout 100</pre>
Verification	Run the show command on the CPE to check whether the configuration commands have been successfully applied.
CPE	<pre>QTECH#show cwmp configuration CWMP Status : enable CPE wait timeout : 100s</pre>

Common Errors

N/A

7.5. Monitoring

Displaying

Command	Function
show cwmp configuration	Displays the CWMP configuration.
show cwmp status	Displays the CWMP running status.

8. CONFIGURING CA-MONITOR

8.1. Overview

Intelligent monitoring is the intelligent hardware management of devices, including intelligent power management, intelligent fan speed adjustment, and intelligent temperature monitoring. The intelligent monitoring performs the following tasks:

- Chassis power monitoring;
- Power-on/-off and power monitoring of line cards
- Automatic fan speed adjustment based on ambient temperature changes
- Real-time temperature monitoring of line cards to alert users
- Automatic power-off of line cards to protect the device when the temperatures of line cards exceed the highest temperature allowed for the device.

By default, the intelligent monitoring function is enabled after the device is powered on. It does not require any manual configuration. Apart from the default configuration, the system provides a variety of configuration methods so that you can change the default configuration of the system as necessary.

Protocols and Standards

N/A

8.2. Applications

Application	Scenario
<u>Power-On/Power-Off</u>	Configures power supply priority for line cards to be powered on/off automatically.
<u>Intelligent Speed Adjustment of Fan</u>	Configures fan operating modes, including standard (default), quiet, and user-defined.
<u>Intelligent Temperature Monitoring</u>	Configures temperature threshold.

8.2.1. Power-On/Power-Off

Scenario

The power supply priorities of line cards refer to the power-on/power-off priorities of the line cards. A line card with a higher power supply priority is powered on at an earlier time, and powered off at a later time. The default power supply priorities of the line cards are as follows:

supervisor module > FE card > VSL card > line card. For the same type of line cards, a line card in a slot with a smaller slot number has a higher priority.

Deployment

N/A

8.2.2. Intelligent Speed Adjustment of Fan

Scenario

The device uses intelligent fans for heat dissipation. The rotating speed of fans is automatically adjusted as the ambient temperature changes to achieve the best heat dissipation effect. When the ambient temperature is low, the rotating speed of fans is kept low to reduce power consumption and noise.

A fan tray can operate in one of the following three modes:

- **Standard mode:** It is the default operating mode. The fans initially run at intermediate speed. As the ambient temperature changes, the rotating speed of the fans automatically decreases or increases to achieve the best heat dissipation effect.
- **Quiet mode:** The fans initially run at relatively low speed. As the ambient temperature changes, the rotating speed of the fans automatically decreases or increases. In this mode, the rotating speed of the fans is lower than that of a fan in standard mode. Therefore, in quiet mode, fans' noise is further reduced.
- **User-defined mode:** In this mode, you will define the rotating speed of the fans and the rotating speed of all the fan trays is the same (at the value defined by yourself). The user-defined mode supports seven levels of rotating speed as listed in Table 8-1. The higher the level, the higher the rotating speed. When you switch the fans to the user-defined mode, if the rotating speed level is not specified, the rotating speed level is 3 by default.

Table 8-1 Definitions of rotating speed levels of fans in user-defined mode

Rotating Speed Level	Rotating Speed (Percentage Relative to the Highest Rotating Speed of Fans)
1	40%
2	50%
3	60%
4	70%
5	80%
6	90%
7	100%

👉 The rotating speed of fans in user-defined mode is fixed. It can be set according to the level defined by users and will not automatically change as the temperature changes. Therefore, the standard mode or quiet mode is recommended so that the rotating speed of fans will automatically change as the temperature changes to protect the device from over-temperature which may cause a fault of the device.

Deployment

N/A

8.2.3. Intelligent Temperature Monitoring

Scenario

Each line card of the device has five temperature detection points: air inlet, air outlet, CPU, and two hottest points on the line card. Some line cards (such as a multi-service card) contain two CPUs, both of which will be monitored. Additionally, the MAC temperatures of the line cards and FE cards should also be monitored. Two temperature thresholds, which are an alarm threshold and a hazard threshold, can be configured for these temperature points. The two temperature thresholds are defined as follows:

- Alarm threshold: When the temperature of the line card exceeds the alarm threshold, the active supervisor module generates a Syslog message and the Alarm LED on the panel becomes yellow.
- Hazard threshold: It indicates the power-off temperature. When the temperature of the line card exceeds the hazard threshold, the line card powers off automatically. In addition, the active supervisor module generates a Syslog message and the Alarm LED on the panel becomes red.

👉 There is no alarm threshold for the CPU temperature and MAC temperature, but only hazard thresholds are defined for them. Only the supervisor module temperature involves both an alarm threshold and a hazard threshold.

The temperature monitoring points are classified into three types:

- Supervisor module temperature: The temperature monitoring points cover the temperatures of air inlet, air outlet, CPU, and hottest pints on the line card
- CPU temperature: CPU temperature of the line card. Each line card has at least one CPU.
- MAC temperature: The engine does not involve the MAC temperature. Each line card or FE card involves at least one MAC temperature.

You can set the thresholds for the preceding three types of temperatures. The thresholds are applied to the chassis only. All the line cards in one piece of chassis share one set of temperature thresholds. The system provides a set of default thresholds. You can keep them

or change them on demand. You must, however, comply with the following rules to set the thresholds:

- The alarm threshold must be lower than the hazard threshold.
- The hazard threshold of the supervisor module temperature cannot exceed 90°C. The hazard thresholds of the CPU and MAC temperatures cannot exceed 110°C.

✎ The alarm threshold of the supervisor module temperature is 56°C and the hazard threshold is 80°C; the hazard threshold of the CPU and MAC temperatures is 100°C, and the CPU and MAC temperatures do not involve any alarm threshold by default.

The system monitors the temperature every two minutes. Once the system discovers that a temperature of the line card exceeds the current alarm threshold, a Syslog message is generated and the Alarm LED on the panel of the active supervisor module becomes yellow. If temperature of the line card exceeds the current hazard threshold, a Syslog message is generated and the Alarm LED becomes red, and the line card is powered off.

✎ When you set a temperature threshold, the system does not judge the lower limit of the threshold. Therefore, the user-configured temperature threshold cannot be excessively small. Otherwise, the system may frequently generate Syslog messages or power off the line card, affecting the normal use of the device. Generally, it is recommended that the lower limit of the alarm threshold of the supervisor module temperature should be 50°C; the lower limit of the hazard threshold of the supervisor module temperature should be 80°C; the lower limit of the hazard threshold of the CPU and MAC temperatures should be 90°C.

Deployment

N/A

8.3. Features

Basic Concepts

→ Operating Mode of the Power Supply

The power supply can operate in one of the following two modes: non-redundancy mode and N+M redundancy mode.

- Non-redundancy mode: It is also called the superposition mode. The power supply operates in non-redundancy mode by default. In this mode, the total power of the system is the sum of power of all power modules.
- N+M redundancy mode: The system has N+M power modules in total, where M indicates the number of configured redundant power modules and N indicates the number of available power modules of the system. The total power of the system is the sum of output power of the N power modules.

→ Power Supply Priority

The power supply priorities of line cards refer to the power-on/power-off priorities of the line cards. A line card with a higher power supply priority is powered on at an earlier time, and powered off at a later time. When the system power is insufficient and thus some line cards need to be powered off, a line card with the lowest priority is powered off first. The default power supply priorities of the line cards are as follows: supervisor module > FE card > VSL card > line card. For the same type of line cards, a line card in a slot with a smaller slot number has a higher priority. You can change the power supply priorities of the line cards only. The power supply priority of a line card ranges from 1 to 16, where 1 indicates the lowest priority and 16 the highest priority.

→ Operating Mode of Fans

A fan tray can operate in one of the following three modes:

- Standard mode: It is the default operating mode. The fans initially run at intermediate speed. As the ambient temperature changes, the rotating speed of the fans automatically decreases or increases to achieve the best heat dissipation effect.
- Quiet mode: The fans initially run at relatively low speed. As the ambient temperature changes, the rotating speed of the fans automatically decreases or increases. In this mode, the rotating speed of the fans is lower than that of a fan in standard mode. Therefore, in quiet mode, fans' noise is further reduced.
- User-defined mode: In this mode, you will define the rotating speed of the fans and the rotating speed of all the fan trays is the same (at the value defined by yourself). Seven levels of rotating speed are available.

↘ In VSU mode, the fans in the two chassis operate in the same working mode.

→ Temperature Threshold

During temperature monitoring, if the temperature reaches a certain threshold, the system takes a corresponding action. For example, if the temperature reaches an alarm threshold, the system generates a Syslog alarm. If the temperature reaches a hazard threshold, the corresponding line card is powered off.

Overview

Feature	Function
<u>Automatic Power-Off of Line Cards</u>	Some line cards are powered off automatically based on priorities in the case of power deficiency.

<u>Manual Power-On/Power-Off of Line Cards</u>	You can manually power on/off some line cards.
<u>Intelligent Speed Adjustment of Fans</u>	The rotating speed of fans is automatically adjusted as the temperature changes to address the heat dissipation needs of the system.
<u>Intelligent Temperature Monitoring</u>	The system automatically monitors the temperature of the line card in each slot. When the temperature exceeds a certain threshold, the system automatically generates an alarm or powers off the line card.

8.3.1. Automatic Power-Off of Line Cards

The line cards with higher priority are power on preferentially in the case of energy deficiency.

[Working Principle](#)

This function enables line cards with higher priority to be powered on preferentially in the case of power deficiency.

Use the **power priority** [**switch devid**] **slot slotid prio** command to configure the priority and the **power priority save** command to save the priority before restarting the device.

[Related Configuration](#)

→ Saving Power Supply Priority

Use the **power priority save** command to save the power supply priority.

👉 Make sure to save the power supply priority after importing config files.

8.3.2. Manual Power-On/Power-Off of Line Cards

You can run the **power off / power on** command to manually power off/on a line card.

👉 Do not manually power off the active supervisor module of the chassis. If you attempt to specify a line card as the active supervisor module of the chassis, the system prompts an error. In VSU mode, the local active supervisor modules in the two chassis cannot be manually powered off.

[Working Principle](#)

You can run the **power off / power on** command to manually power off/on a line card. You can also run the power cycle command to enable auto power-on for a line card after a certain period of powered-off.

[Related Configuration](#)

N/A

8.3.3. Intelligent Speed Adjustment of Fans

When the fans work in standard or quiet mode, the rotating speed is automatically adjusted as the temperature changes.

Working Principle

The system automatically specifies default start rotating speed for the fans according to the current operating mode of the fans. As the ambient temperature rises or drops, the fans automatically raise or reduce their rotating speed to dissipate heat and ensure that the noise is low.

The system provides a user-defined mode in which all the fans operate at user-specified rotating speed. In user-defined mode, the rotating speed of fans is fixed and not adjusted as the ambient temperature changes. It is recommended to configure the fans with standard or quiet mode to protect them from over-temperature.

Related Configuration

→ Changing the Operating Mode of Fans

The fans operate in standard mode by default.

You can use the **fan mode** command to change the operating mode of the fans to standard mode, quiet mode, or user-defined mode.

8.3.4. Intelligent Temperature Monitoring

The supervisor module monitors the temperature of all line cards and notifies users of temperature change.

Working Principle

The system defines three types of temperature, including supervisor module temperature, CPU temperature and MAC temperature, and two thresholds, namely, alarm threshold and hazard threshold. There is no alarm threshold for the CPU temperature and MAC temperature, but only hazard thresholds are defined for them. Only the supervisor module temperature involves both an alarm threshold and a hazard threshold. The system monitors the temperature every two minutes. Once the system discovers that a temperature of the line card exceeds the current alarm threshold, a Syslog message is generated and the Alarm LED on the panel of the active supervisor module becomes yellow. If temperature of the line card exceeds the current hazard threshold, a Syslog message is generated and the Alarm LED becomes red, and the line card is powered off.

↪ The active supervisor module in the chassis or the global active supervisor module in VSU mode generates a Syslog message when discovering that its temperature exceeds the hazard threshold. At the same time, the Alarm LED on the panel becomes red. However, the active supervisor module or global active supervisor module will not automatically power off. In this case, you need to take effective measures to cool the active supervisor module or manually remove the active supervisor module for cooling.

Related Configuration

→ Changing Temperature Thresholds


By default, the alarm threshold of the supervisor module temperature is 56°C and the hazard threshold is 80°C; the hazard thresholds of the CPU temperature and MAC temperature are 100°C.

You can use the **threshold set temperature [switch *devid*] { board | cpu | mac } { warning | shutdown } temp** command to change the thresholds of the supervisor module temperature, CPU temperature, and MAC temperature.

- 👉 The configured alarm threshold of the supervisor module temperature must be lower than the current hazard threshold. Otherwise, the configuration fails.
- 👉 The configured hazard threshold of the supervisor module temperature cannot exceed 90°C, and that of the CPU temperature and MAC temperature cannot exceed 110°C. Otherwise, the configuration fails.

8.4. Configuration

Configuration	Description and Command
Configuring Line Card Power-On/Power-Off	👉 The configuration here is optional. It is used to configure power-on/-off of the line card.
	power priority Sets the power supply priority of a line card.
	power Powers on or off the specified line card.
	power cycle Powers off the specified line card, and then powers it on. You can specify the time interval between the power-off and the next power-on. The default interval is 1 second.
Configuring the Operating Mode of Fans	👉 The configuration here is optional. It is used to change the operating mode of fans.
	fan mode Sets the fans to the standard mode, quiet mode or user-defined mode.

<u>Configuring Temperature Thresholds</u>	<p> The configuration here is optional. It is used to change temperature thresholds.</p>	
	threshold set temperature	Sets the alarm threshold and hazard threshold of the supervisor module temperature, or the hazard thresholds of the CPU temperature and MAC temperature.

8.4.1. Configuring Power-On/Power-Off of Line Cards

Configuration Effect

- Change the power-on/power-off priorities of line cards.
- Power on or off the specified line card.
- Power off the specified line card first, and then power it on.

Notes

- The active supervisor module of the chassis cannot be specified for power off. In VSU mode, the local active supervisor modules in the two chassis cannot be specified for power off.

Configuration Steps

The configuration here is optional.

Verification

- Use the **show power priority** command to display the power-on/power-off priority of a line card and check whether the automatic power-off function is enabled on the line card.
- Use the **show power** command to display the current power supply status of each line card.

Related Commands

→ Configuring the Power Supply Priority of a Line Card

Command	power priority [switch devid] slot slotid prio
Parameter Description	<p>switch devid: It is supported in VSU mode only. It specifies the chassis No. of the line card whose power-on/power-off priority is to be configured. By default, it refers to the current chassis.</p> <p>slot slotid: It specifies the slot No. of the line card whose power-on/power-off priority is to be configured. Depending on the chassis type, a chassis may have 3 slots, 5 slots, 8 slots, or 12 slots.</p> <p>prio: It specifies the line card priority to be set, ranging from 1 to 16, where 1 indicates the lowest priority and 16 the highest priority.</p>
Command Mode	Global configuration mode

Usage Guide	This command is used to change the default power supply priority of a line card or VSL card. The power supply priority of an FE card is defined by default, which cannot be changed.
--------------------	--

→ Powering On/Off the Specified Line card

Command	power { on off } [switch <i>deviid</i>] slot <i>slotid</i>
Parameter Description	on: Powers on the specified line card. off: Powers off the specified line card. switch <i>deviid</i>: It is supported in VSU mode only. It specifies the chassis No. of the line card to be powered on/off. By default, it refers to the current chassis. slot <i>slotid</i>: It specifies the slot No. of the line card to be powered on/off. The supervisor modules are inserted in M1 and M2 slots. The FE cards are inserted in FE1, FE2, FE3, and FE4 slots.
Configuration Mode	Global configuration mode
Usage Guide	N/A

→ Powering Off the Specified Line card and then Powering It On

Command	power cycle [switch <i>deviid</i>] slot <i>slotid</i> [interval <i>seconds</i>]
Parameter Description	switch <i>deviid</i>: It is supported in VSU mode only. It specifies the chassis No. of the line card to be powered on/off. By default, it refers to the current chassis. slot <i>slotid</i>: It specifies the slot No. of the line card to be powered on/off. The supervisor modules are inserted in M1 and M2 slots. The FE cards are inserted in FE1, FE2, FE3, and FE4 slots. interval <i>seconds</i>: It specifies the time interval between power-off and the next power-on. The default interval is one second.
Configuration Mode	Global configuration mode
Usage Guide	N/A

Common Errors

N/A.

8.4.2. Configuring the Operating Mode of Fans

Configuration Effect

- You can use the **fan mode** command to change the operating mode of the fans to standard mode, quiet mode, or user-defined mode. The default mode is standard.

Notes

N/A

Configuration Steps

- The configuration here is optional.

- The fans operate in standard mode by default. You can switch the fans to the quiet or user-defined mode.

Verification

- Use the **show fan** command to display the operating mode of all the fan trays.
- Use the **show fan detail** command to display the actual rotating speed of the internal small fans in each fan tray.

Related Commands

→ Configuring the Operating Mode of Fans

Command	fan mode { normal quiet { defined [speed-level level] }}
Parameter Description	<p>normal: It indicates that the fans operate in standard mode, which is the default operating mode.</p> <p>quiet: It indicates that the fans operate in quiet mode.</p> <p>defined: It indicates that the fans operate in user-defined mode. In user-defined mode, the rotating speed of each fan in the fan trays of the chassis is the same, which will not change as the system temperature changes. Therefore, the user-defined mode is not recommended.</p> <p>speed-level level: In user-defined mode, it specifies the rotating speed level of the fans. Seven levels are available; that is, the value of level ranges from 1 to 7. The rotating speed level is level 3 by default.</p>
Configuration Mode	Global configuration mode

Configuration Examples

Configuration Steps	<ul style="list-style-type: none"> • Set the fans to the quiet mode.
	<pre>QTECH(config)#fan mode quiet</pre>
Verification	<p>Use the show fan command to check the current operating mode of the fans.</p> <ul style="list-style-type: none"> • Check whether the operating mode of the fans has been switched successfully.
	<pre>QTECH#show fan Chassis-type: QSW-7605 Fan-id: 1 Fan-type: QSW-M05_FAN Serial Number: 1234567890123 Energy-saving: off fan-id status mode speed-level ----- - 1 ok quiet N/A</pre>

Common Errors

- If the ambient temperature changes greatly and you choose the user-defined mode, the rotating speed of the fans cannot be adjusted intelligently, causing a poor heat dissipation effect.

8.4.3. Configuring Temperature Thresholds

Configuration Effect

- Set the alarm thresholds and hazard thresholds of temperature.

Notes

- Set temperature thresholds according to the chassis configuration. All line cards in of the same chassis share the same set of thresholds.

Configuration Steps

- The configuration here is optional.
- You can keep the default temperature thresholds or change them by running corresponding commands.

Verification

- Use the **show temperature** command to check the temperature thresholds and the current temperature of each line card.

Related Commands

→ Configuring Temperature Thresholds

Command	threshold set temperature [switch <i>devid</i>] { board cpu mac } {warning shutdown } temp
Parameter Description	switch <i>devid</i> : It is supported in VSU mode only. It specifies the chassis No. of the line card whose temperature thresholds are to be configured. By default, it refers to the current switch. board : It specifies the temperature thresholds of the supervisor module, including the temperatures of the air inlet, air outlet, and the hottest points on the supervisor module. The temperature thresholds of the supervisor modules are the same for all the line cards. cpu : It specifies the CPU temperature thresholds. The CPU temperature thresholds are the same for all the line cards. mac : It specifies the MAC temperature thresholds. The MAC temperature thresholds are the same for all the line cards. warning : It specifies the alarm threshold of the line card temperature. When the temperature detection point is cpu or mac , this key word is invisible. shutdown : It specifies the hazard threshold (that is, the power-off threshold) of the line card temperature. temp : It specifies the temperature threshold value to be set.
Configuration Mode	Global configuration mode
Usage Guide	N/A

Configuration Examples

→ Setting the Alarm Threshold of the Supervisor module Temperature of the VSU Device to 75°C

Configurati on Steps	<ul style="list-style-type: none"> ● Set the alarm threshold of the supervisor module temperature of chassis 1. ● Set the alarm threshold of the supervisor module temperature of chassis 2.
	<pre>QTECH(config)#threshold set temperature switch 1 board warning 75 QTECH(config)#threshold set temperature switch 2 board warning 75</pre>
Verification	<p>Use the show temperature command to check the alarm and hazard thresholds of the current line card.</p> <ul style="list-style-type: none"> ● Check the alarm threshold of the supervisor module temperature to determine whether the alarm threshold settings have taken effect.
	<pre>QTECH#show temperature slot card_type warning(C) shutdown(C) current(C) ----- ----- 1/1 N/A N/A N/A N/A 1/2 QSW-M7600-48GT4XS-EB 75 80 100 100 30 31 37 40 (N/A) (N/A) 1/3 N/A N/A N/A N/A 1/M1 QSW-M7608-CM 75 80 100 100 22 31 25 31 (35) (N/A) 1/M2 QSW-M7608-CM 75 80 100 100 23 29 25 29 (34) (N/A)</pre>

Common Errors

- When the thresholds exceed the allowed values, the threshold settings are invalid.
- When the alarm thresholds are excessively low, the system frequently generates alarm logs.

8.5. Monitoring

Displaying

Command	Function
show power [priority version]	Displays power information about line cards and respective power supply priorities

show fan [{ [[<i>devid</i>] <i>fanid</i>] detail } version]	Displays fan information
show temperature	Displays line card information such as current temperature and temperature thresholds

9. CONFIGURING SOFTWARE AUTHORIZATION MANAGEMENT

9.1. Overview

Software authorization is an intermediate link for users to use some extension functions of the device. A user can use the extension functions after installing correct license files. The extension functions provided by RGOS include the VSD, TRILL, FCoE, and number of concurrent users supported by SSLVPN. A user can use general functions and extension functions of the RGOS after being authorized.

- ↳ Generally, all features of the RGOS are installed for the device before delivery of the device. However, users cannot use some features of the RGOS before they obtain a corresponding license file.
- ↳ Whether a feature requires authorization and the authorization type are specified in the configuration guide of the feature. Unless otherwise specified, basic functions of the system can be used without authorization.

9.2. Typical Application

9.2.1. VSD

Application Scenario

VSD is a network system virtualization technology. It is used to divide one physical device into multiple logical devices by means of virtualization. In addition, VSD makes use of existing resources to the maximum extent, reducing the network operation cost.

Before being authorized, a user can only use VSD0 (that is, common CLI). After being authorized, the user can create other VSDs.

Function Deployment

The authorization module only functions on VSD0. License files cannot be installed on other VSDs.

9.2.1. FCoE

Application Scenario

The FCoE technology can map the fiber channel to the Ethernet and insert the fiber channel information into the Ethernet information packet to enable SAN data transmission over the Ethernet instead of over the fiber channel connecting the server to the SAN storage device.

Before the FCoE license file is installed on the device, the FCoE is not available. After the FCoE license file is installed, users can use the FCoE.

Function Deployment

-

9.3. Function Details

Basic Concept

→ License File for a Feature

A license for a certain special feature obtained by means of license file, hardware entity, or legal contract. This license stipulates the maximum number of users allowed to use it, the maximum number of instances allowed to be used, and validity period.

→ Authorized Software

Software function that can be used after being authorized.

→ Host Number

Unique serial number for identifying each device.

👉 In VSU environment, a license can adopt the host ID of any chassis. When the chassis exits the VSU environment, the feature corresponding to the license becomes invalid.

→ Authorization by Products

One license file is applied to only one device, which matches the host number. License file migration is not supported.

→ Purchase Voucher

Purchase voucher of a license file. This voucher contains the product activation key (PAK) and the website for downloading the license file.

→ Product Activation Key (PAK)

The legal owner of the purchase voucher logs in to the website (listed on the purchase voucher) for downloading the license file and uses the PAK for registration. After that, a corresponding license file is provided on the webpage for downloading or directly sent to the registered mailbox.

→ License File

After a license file is installed on a device, users can use relevant functions. Each license file contains a digital signature to avoid manipulation. A license file is used for authorization based on products.

→ License Stacking

Different license files can be used on one device. For example, if a device provides both the FCoE and TRILL functions, users can purchase the license files of the two functions and use them on the same device.

→ Temporary License File

A temporary license file becomes invalid after a period of time.

→ Evaluation License File

Evaluation license file belongs to temporary license file. Generally, an evaluation license file is installed on a device before delivery, and it is mainly used to provide users with the function of using a certain trial feature. This type of license file is independent of the host number.

→ Permanent License File

A permanent license file is permanently valid.

→ Single-Instance License File

Only one license file can be installed for a feature at a time.

☞ Currently, the license file for the feature like the number of concurrent users supported by VSD, TRILL, FCoE, and SSLVPN is a single-instance license file.

→ Multi-Instance License File

Multiple license files can be installed for the same feature on a device.

☞ Currently, only the license file for the feature "number of users supported by the AP" is a multi-instance license file.

→ Friendly Period Warning

Friendly period warning is issued in log or TRAP form several days before the license file expires. Friendly period warning is set to prevent a license file with a validity period from stopping working suddenly when the validity period expires, ensuring network performance.

Functions and Features

Function and Feature	Description
Obtaining and Using a License File	Describe how to obtain and use a license file.
Backing Up, Updating, and Removing a License File	Describe how to back up, update, and remove a license file.

9.3.1. Obtaining and Using a License File

→ Using the License File

A license file must be purchased from the website or marketing channel of QTECH for formal authorization. Authorization is based on each device. To obtain a license file, visit the website on the purchase voucher and provide the PAK and host ID. The license file can be directly downloaded by a user or sent to a user by email. After obtaining the license file, users need to install the license file. After installing the license file, users can use the features corresponding to the license file.

The license files of the RGOS include permanent license file and temporary license file (evaluation license file is a type of temporary license file). Once a user starts using a temporary license for a certain feature, timekeeping is started for this license file, and this feature is disabled after the validity period of the license file expires. To continue using this feature, this user can purchase another license file (permanent or temporary license file) from the website or marketing channel of QTECH.

👉 In the VSU environment, multiple devices form one virtual device. In this scenario, as long as one device obtains the license file for a certain feature, the VSU obtains the license file for this feature. However, when these devices are used separately again, authorization is still based on each device.

👉 The VSD function provided by RGOS helps to divide one RGOS device into multiple virtual devices. For users, each virtual device seems like an independent device. In this environment, license files are managed in global configuration mode. That is, when the license file for a certain feature is obtained, the license files for this feature in all VSD domains are obtained. In addition, license files are installed and managed in the default VSD exclusively.

→ Check of the License File

After a device starts to run, the license file for each authorized feature needs to be checked. If the corresponding license file is properly installed, this feature is ready for application. Otherwise, this feature becomes invalid and cannot be used.

👉 Checking the license files for various features occurs at different times. That is, the license files for some features are checked during startup, and the license files for some features are checked in real time.

→ Loss of the License File

License files are stored in the **data** directory of a device and will not be lost after software upgrade.

If the memory or file system is damaged with the license file backed up, you can install the backup license file again after system recovery. If the license file is not backed up, you can visit the authorization website of QTECH and obtain the license file again. The process of regaining

the license file is the same as the process of obtaining a new license file (you do not need to purchase the license file again).

Authorization is based on each device. After a license file is provided for a specified device, authorization via this license file can be conducted on this device exclusively. The host ID may change during device maintenance or replacement. In case of host ID change, the license file obtained before can no longer be identified. In this case, contact the after-sales engineers of QTECH.

9.3.2. Backing Up, Updating, and Removing a License File

→ Backing Up a License File

In case that a fault such as file system storage media damage occurs on a device, the license file on this device may be lost after you rectify this fault. Therefore, you need to back up the license file for reinstallation in case of a fault.

→ Updating a License File

If the existing license file in the system cannot meet users' requirements for a feature, users can visit the website of QTECH to purchase a license file and then update the license file locally.

→ Removing a License File

If a feature is not needed, the user can remove the license file for this feature to improve the utilization rate of various resources like the memory. If the user want to use this feature again after removing its license file, t reinstall the license file. It is recommended that license files be kept properly.

9.4. Configuration Details

Configuration Item	Configuration Suggestion & Relevant Command	
Basic Functions of Software Authentication	👉 Mandatory configuration. Installs a license file.	
	<code>show license hostid</code>	Obtains the host ID of the device.
	<code>license install</code>	Installs a license file manually.
Backing Up License File	👉 Optional configuration. Backs up a license file.	
	<code>license copy</code>	Backs up a license file.
Friendly Period Warning	👉 Optional configuration. Sets the time of issuing a warning before the validity period of a license file expires.	
	<code>license grace-peroid</code>	Sets a friendly period warning.

<u>Updating License File</u>	Optional configuration. Updates an existing license file on the device.	
	license update	Updates a license file.
<u>Removing License File</u>	Optional configuration. Removes an existing license file on the device.	
	license uninstall	Removes a license file manually.
<u>Unbinding License</u>	Optional configuration. Unbinds the license on the device.	
	license unbind	Unbinds the license.

9.4.1. Basic Functions of Software Authorization

Configuration Effect

A license file is installed to enable the corresponding function.

Notes

- After downloading a license file from a specified website, upload this license file to the device (or store it in a USB flash drive) for installation. You don't need to connect the device to the Internet during the installation.
- Different devices cannot share the same license file.
- After a license file is installed on a device, this license file is automatically backed up in the data directory of the system (the name of a license file ends with ".lic"). When you remove a license file, the backup file of this license file is also removed.

Configuration Steps

→ Obtaining Host ID of the Device

- Mandatory configuration.
- host-id indicates the host ID.
- If you want to apply a feature requiring authorization without installing the license file, the CLI displays a prompt indicating that the unauthorized feature is unavailable and provides the website for downloading the license file.

Command	show license hostid
Parameter Description	N/A
Command Mode	Privileged EXEC mode

Usage Guide	<ul style="list-style-type: none"> ✎ The name of a license file cannot be modified. ✎ This command does not require license.
--------------------	--

→ Obtaining the PAK

- Mandatory configuration.
- Generally, a PAK is provided in a paper purchase voucher by QTECH after a user purchases a license file.

→ Obtaining the License File of the Product from QTECH Web URL

- Mandatory configuration.
- After logging in to the authorization website, you can obtain the license file according to the prompts.

→ Copying the License File to the File System of the Device

- Mandatory configuration.
- Use conventional file system operation commands to perform this operation. For example, download the license file through the TFTP protocol or copy the license file to a USB flash drive.

→ Installing the License File

- Optional. You can use the **license-install** command to install a license file.

✎ If you use the **license install** command in the VSU environment, the whole VSU is configured with the feature corresponding to the license file as long as one device obtains that feature. Once the devices are separated, the license takes effect on only the device configured with the command.

✎ In the VSD environment, license files are managed in global configuration mode. That is, when the license file for a certain feature is obtained, the license files for this feature in all VSD domains are obtained. In addition, license files are installed and managed in the default VSD exclusively.

Command	license install { flash: usb0: } filename
Parameter Description	flash: Specifies that the license file is installed in the internal flash file system. usb0: Specifies that the license file is installed in the USB file system. filename: Specifies the name of the license file.
Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Verification

- You can run the **show license all_license** command to check the license name. If the license name is displayed, the corresponding license file is installed.

Command	show license { all_license file [license] }
Parameter Description	all_license: Displays all license files already installed on the device. file filename: Displays a specified license file.
Command Mode	Privileged EXEC mode
Usage Guide	Users can check whether a license file is installed by checking the feature name.
Verification	<pre>QTECH(config)#show license all-license Searching license in the system... 1. Service name: LIC-FCoE Attribute: Permanent, Single_instance, Releasable Licensed serial number: LIC-FCOE00000012268889 2. Service name: LIC-VSD Attribute: Temporary, Single_instance, Releasable Left days: 362 Licensed serial number: LIC-VSD00000012268888</pre>

Configuration Examples

→ Installing a VSD License File in non-VSU environment

Network Environment	To enable the VSD function
Configuration Steps	<ul style="list-style-type: none"> Run the show license hostid command to obtain the host ID of the device. Register at the authorization website, and perform operation based on the prompts to obtain the license file vsd.lic for the VSD feature (the host ID of the device and PAK are required). The detailed operation is omitted in this example. Store the vsd.lic file in a USB flash drive, and connect the USB flash drive to the device. Install the vsd.lic file.
	<pre>QTECH#show license hostid 8708EH5F00042 QTECH#license install usb0:vsd.lic</pre>

	License file install success, service name: LIC-VSD.
Verification	Run the show license all_license command to check the license name. If the license name is displayed, the corresponding license file is installed..
	<pre>QTECH(config)#show license all-license Searching license in the system... 1.Service name: LIC-VSD Attribute: Temporary, Single instance, Releasable Left days: 362 Licensed serial number: LIC-VSD00000012268888</pre>

Common Errors

- Install a license file that does not belong to the present device.
- No matching device is available.
- Reinstall a license file.
- Install a license file with its later version installed in the system.

9.4.2. Backing Up License File

Configuration Effect

- The license files of one or all features in the system are backed up.

Notes

- The license file of the evaluation version must not be backed up.
- License files can be backed up only when sufficient storage space is available.

↳ Generally, one license file occupies a space ranging from 4 KB to 10 KB.

Configuration Steps

→ Backing Up a License File of the System

- The backup license file is a regular file.
- When you back up all license files in the system, a tar file is generated.

Command	license { copy-all copy-file filename } { flash: usb0: } [target-filename]
Parameter Description	<p>copy-all: Copies all permanent license files in the system.</p> <p>copy-file filename: Copies the filename license file in the system. filename can be the name of a license file already installed in the system or the name of a feature. When filename is a feature name, all license files already installed for this feature are backed up.</p> <p>flash: Specifies that the license file is installed in the internal flash file system.</p> <p>usb0: Specifies that the license file is installed in the USB file system.</p> <p>filename: Specifies the name of the license file.</p>
Defaults	N/A

Command Mode	Privileged EXEC mode
Usage Guide	N/A

→ Uploading a License File to Another System for Storage

- You can use a file system management command to further save a license file to other storage devices, such as a USB flash drive.

Verification

- You can run the `dir` command to check whether the license file backup is generated. In addition, you can check whether the backup is correct by comparing the output of the `dir` command with the license file name in the installed license field of the feature with permanent authorization displayed by running the `show license all-license` command.

Command	<code>dir [filesystem:] [file-url]</code>
Parameter Description	<i>filesystem</i> : The file system URL followed by a colon. The file systems include <code>flash:</code> , <code>usb:</code> , and <code>tmp:</code> . <i>file-url</i> : Path name. The path starting with "/" indicates an absolute path. Otherwise, it is a relative path.
Command Mode	Privileged EXEC mode
Usage Guide	This command does not require license.
Verification	<pre> QTECH#dir usb0:rg-license-lics Directory of usb0:/rg-license-lics 1 drwx 4096 Fri Jun 20 12:29:32 2014 . 2 drwx 4096 Fri Jun 20 12:28:37 2014 .. 3 -rwx 8704 Fri Jun 20 12:29:12 2014 lics.tar 1 file, 2 directories 536870912 bytes total (740,687,872 bytes free) </pre>

Command	<code>show license { all-license file [license] }</code>
Parameter Description	all-license : Displays all license files already installed on the device. file filename : Displays a specified license file.
Command Mode	Privileged EXEC mode
Usage Guide	Users can check whether a license file is installed by checking the feature name.

	<p>☞ Only a multi-instance license file has the installed license field. The multi-instance license file backup is named after the ID of the multi-instance license file. At most one single-instance license file exists in the system at a time; therefore, the single-instance license file backup is named after the feature.</p>
Verification	<pre>QTECH#show license all-license Searching license in the system... Service name: LIC-FCoE Attribute: Permanent, Single_instance, Releasable Licensed serial number: LIC-FCOE00000012268889 2. Service name: LIC-VSD Attribute: Temporary, Single_instance, Releasable Left days: 362 Licensed serial number: LIC-VSD00000012268888 3. Service name: LIC-AP-64 Attribute: Permanent, Multiple_instance, Releasable [Installed licenses] [Licensed serial number] 19881021.lic LIC-AP-6400000012264966 19881023.lic LIC-AP-6400000012264988</pre>

Configuration Examples

→ Backing Up All License Files of the System

Network Environment	Back up all license files in the system and name the backup lics.tar.
Configuration Steps	<ul style="list-style-type: none"> ● Connect a USB flash drive to the device. ● Back up all permanent license files in the USB flash drive and name the backup lics.tar.
	<pre>QTECH#lic copy-all usb0:rg-license-lics/lics.tar Success to copy all permanent license.</pre>
Verification	<ul style="list-style-type: none"> ● You can run the dir command to check whether the license file package is generated. After decompressing the package, you can check whether the backup is correct by comparing the files in the package with the license file name displayed in the installed license field of the feature with permanent authorization displayed by running the show license all-license command.

- ☞ Only a multi-instance license file has the installed license field. The multi-instance license file backup is named after the ID of the multi-instance license file. At most one single-instance license file exists in the system at a time; therefore, the internal single-instance license file backup is named after the feature.
- ☞ In this example, the IDs 19881021.lic and 19881023.lic are embedded in the license file. License files are stored in different folders based on the features during the packing; therefore, users can still identify the mapping between license files and features.

```

QTECH#dir usb0:rg-license-lics
Directory of usb0:/rg-license-lics
  1 drwx          4096  Fri Jun 20 12:29:32 2014  .
  2 drwx          4096  Fri Jun 20 12:28:37 2014  ..
  3 -rwx          8704  Fri Jun 20 12:29:12 2014  lics.tar
1 file, 2 directories
536870912 bytes total (740,687,872 bytes free)
QTECH#show license all-license
Searching license in the system...
1. Service name: LIC-FCoE
Attribute: Permanent, Single_instance, Releasable
Licensed serial number: LIC-FCOE00000012268889
2. Service name: LIC-VSD
Attribute: Temporary, Single_instance, Releasable
Left days: 362
Licensed serial number: LIC-VSD00000012268888
3. Service name: LIC-AP-64
Attribute: Permanent, Multiple_instance, Releasable
[Installed licenses]      [Licensed serial number]
19881021.lic              LIC-AP-6400000012264966
19881023.lic              LIC-AP-6400000012264988

```

Common Errors

- Specify a license file or a file not in the system.
- Specify a temporary license file for backup (a temporary license file cannot be backed up).

9.4.3. Friendly Period Warning

Configuration Effect

- Before the validity period of an evaluation license file expires, a warning is issued in log mode, enabling users to take measures in advance.

Notes

- Each authorized feature should be set separately.
- This setting may be affected by device time adjustment.
- A permanent license file does not need to be configured with friendly period warning.

Configuration Steps

→ Configuring a Friendly Period Warning for an Authorized Feature

Command	license grace-period <i>filename days</i>
Parameter Description	<i>filename</i> : name of the license file for a feature <i>days</i> : The period from the expiry time to the warning time,
Defaults	The default value is the smaller one between 120 and half the evaluation license file's validity period.
Command Mode	Privileged EXEC mode
Usage Guide	-

Verification

- 1: Set the expiry time of a license file to be earlier than the warning time, and the warning is displayed at regular intervals.
- 2: Run the **show license** command to check whether the time of the Alarm starting point filed is consistent with the setting.

Command	show license { all-license file [<i>license</i>] }
Parameter Description	all-license : Displays all license files already installed on the device. file <i>filename</i> : Displays a specified license file.
Command Mode	Privileged EXEC mode
Usage Guide	This command does not require license.
Verification	<pre>QTECH#show license file LIC-VSD Service name: LIC-VSD Attribute: Temporary, Single instance, Releasable Left days: 362 Licensed serial number: LIC-VSD00000012268888</pre>

Configuration Examples

→ Changing the Friendly Period Warning Time

Network Environment	The temporary license file for the VSD feature has already been installed on the device, and the friendly period warning time is set to 100 days.
Configuration Steps	<ul style="list-style-type: none"> Set the friendly period warning time to 100 days.
	<pre>QTECH#lic grace-period LIC-VSD 100 RG_LICENSE: success to set alarm starting point of license LIC-VSD.</pre>
Verification	When the validity period of the license file for the VSD feature is shorter than 100 days, the friendly period warning is displayed at regular intervals.
	<pre>QTECH#*Jun 18 10:06:36: %RG_LICENSE-4-LICENSE_DEADLINE_INFO: Service LIC-VSD will be disabled 80 days behind. In order to avoid the inconvenience to you, please log on website http://192.168.5.227:8080/login.jsf to get a new license.</pre>

Common Errors

- Set friendly period warning for a permanent license file.
- No license file is installed in the preset feature system.

9.4.4. Updating License File

Configuration Effect

- The license file for a feature of the system is updated. Generally, this configuration is performed to update an evaluation license file into a temporary license file.

Notes

- A formal permanent license file does not need to be updated.
- A license file cannot be updated to the earlier version.

⚠ A license file has a time filed. The value of this field is subject to the time when the license file is generated from the website. The later the time, the later the version.

Configuration Steps

→ Updating a License File

- You can run the license update command to update the license file for a feature.
- Update the license file without connecting the device to the Internet.

Command	license update { flash: usb0: } filename
Parameter Description	flash: Specifies that the license file is installed in the internal flash file system. usb0: Specifies that the license file is installed in the USB file system. filename: Specifies the name of the license file.

Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Verification

- You can run the **show license** command and check the Attribute field. If the field is displayed as Permanent, the corresponding attribute is updated.

Command	show license { all-license file [license] }
Parameter Description	all-license: Displays all license files already installed on the device. file filename: Displays a specified license file.
Command Mode	Privileged EXEC mode
Usage Guide	This command does not require license.
Verification	<pre>QTECH#show license all-license Searching license in the system... 1. Service name: LIC-FCoE Attribute: Permanent, Single_instance, Releasable Licensed serial number: LIC-FCOE00000012268889 2. Service name: LIC-VSD Attribute: Temporary, Single_instance, Releasable Left days: 362 Licensed serial number: LIC-VSD00000012268888</pre>

Configuration Examples

→ Updating the VSD License File

Network Environment	Update the temporary license file for VSD in the system to a permanent license file.
Configuration Steps	<ul style="list-style-type: none"> Purchase the permanent license file vsd_perm.lic for VSD, store the vsd_perm.lic file in a USB flash drive, and connect the USB flash drive to the device. Update the license file for VSD.
	<pre>QTECH#license update usb0:vsd_perm.lic</pre>

	License file update success, temporary license LIC-VSD changes into permanent.
Verification	<ul style="list-style-type: none"> You can run the show license command and check the Attribute field. If the field is displayed as Permanent, the corresponding attribute is updated.
	<pre>QTECH(config)#show license all-license Searching license in the system... 1. Service name: LIC-FCoE Attribute: Permanent, Single_instance, Releasable Licensed serial number: LIC-FCOE00000012268889 2. Service name: LIC-VSD Attribute: Permanent, Single_instance, Releasable Licensed serial number: LIC-VSD00000012266666</pre>

Common Errors

- Install a license file that does not belong to the present device.
- Replace the license file of the new version with the old version.
- Reinstall a license file.
- Replace the permanent license file with the temporary license file.
- Start update when the corresponding feature is not installed for the system.

9.4.5. Removing License File

Configuration Effect

- Remove the license files for one or all features in the system.

↪ If a feature is not needed, the user can remove the license file for this feature to improve the utilization rate of various resources like the memory. After being removed, this feature becomes unavailable.

Notes

- If you remove the license file in use, the removal operation takes effect next time when the feature is enabled or restarted.
- To reinstall a license file after removing it, you need to obtain the license file. It is recommended that you back up the license file before removing it.

Configuration Steps

→ Removing a License File from the System

- Run the **license uninstall** command to remove a license file from the system.

Command	license uninstall { all <i>license</i> [<i>filename</i>] }
Parameter Description	all : Remove all license files in the system. <i>license</i> : name of the license file to be removed <i>filename</i> : name of the file to be removed
Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	After you remove the license file for a feature that is running, the license file removal does not take effect immediately. A license file cannot be restored after it is removed. It is recommended that you back up the license file before removing it. This command does not require license.

Verification

- You can run the **show license all-license** command to display the Service name filed. If the name of a feature corresponding to a license file already removed is not displayed, the removal is successful.

Command	show license { all-license file [<i>license</i>] }
Parameter Description	all-license : Displays all license files already installed on the device. file <i>filename</i> : Displays a specified license file.
Command Mode	Privileged EXEC mode
Usage Guide	This command does not require license.
Verification	<pre>QTECH#show license all-license Searching license in the system... 1. Service name: LIC-FCoE Attribute: Permanent, Single_instance, Releasable Licensed serial number: LIC-FCOE00000012268889</pre>

Configuration Examples

→ Removing the VSD License File

Network Environment	Remove the license file for VSD in the system.
Configuration Steps	<ul style="list-style-type: none"> Remove the license file for the VSD feature.
	<pre>QTECH(config)#license uninstall LIC-VSD</pre>

	License file uninstall LIC-VSD success.
Verification	<ul style="list-style-type: none"> Run the show license all-license command to view the Service name filed. If the name of a feature corresponding to a license file already removed is not displayed, the removal is successful.
	<pre>QTECH(config)#show license all-license Searching license in the system... 1. Service name: LIC-FCoE Attribute: Permanent, Single instance, Releasable Licensed serial number: LIC-FCOE00000012268889</pre>

Common e Errors

- The license file has not been installed on the device.
- Specify a license file not on the device.

9.4.6. Unbinding License

Configuration Effect

- Unbind and inactivate a license file.

↪ If you want to unbind a license file on the device, you should unbind the license code on the device first.

Notes

- After the license file is unbound from the device, you will get a verification code, which will be used for the unbinding operation on the authorization website.
- After the license code is unbound, the corresponding license file cannot be installed again.

Configuration Steps

→ Unbinding a License File

- Run the license unbind command to unbind a license file.

Command	license unbind <i>pak</i>
Parameter Description	<i>pak</i> : The license code.
Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	Run the show license all-license to display the installed license code. This command does not require license.

Verification

- Run the **show license all-license** command to display the licensed serial number field. If the license code is not displayed, it indicates that the license is unbound.

Command	show license { all-license file [license] }
Parameter Description	all-license: Displays all license files already installed on the device. file filename: Displays a specified license file.
Command Mode	Privileged EXEC mode
Usage Guide	This command does not require license.

Configuration Example

→ Unbinding License code LIC-VSD00000012268888

Network Environment	The license corresponding to license code LIC-VSD00000012268888 is installed.
Configuration Steps	<ul style="list-style-type: none"> Unbind license code LIC-VSD00000012268888
	<pre>QTECH#license unbind LIC-VSD00000012268888 Success to unbind license LIC-VSD00000012268888. The verification string is: 775719468737BA269825589557F558657575B5D5D5D785782598859765A8355855</pre>
Verification	<ul style="list-style-type: none"> Run the show license all-license command to display the licensed serial number field. If the license code is not displayed, it indicates that the license is unbound.
	<pre>Before Binding QTECH#show license all-license Searching license in the system... 1. Service name: LIC-AP-64 Attribute: Releasable [Permanent licenses] [Licensed serial number] 19880966.lic LIC-AP-6400000012264966 19880988.lic LIC-AP-6400000012264988 [Temporary license] [Licensed serial number] 19880900.lic LIC-AP-6400000012264900 (63 days left) 2. Service name: LIC-VSD</pre>


```

Attribute: Permanent, Releasable
Licensed serial number: LIC-VSD00000012268888
After Binding
QTECH#show license all-license
Searching license in the system...
1. Service name: LIC-AP-64
Attribute: Releasable
[Permanent licenses]      [Licensed serial number]
19880966.lic              LIC-AP-6400000012264966
19880988.lic              LIC-AP-6400000012264988
[Temporary license]      [Licensed serial number]
19880900.lic              LIC-AP-6400000012264900
(63 days left)

```

Common Errors

- No matching license code exists on the system.

9.5. Monitoring and Maintenance

Verifying the License File Configuration

Function	Command
Displays the license configuration.	show license { all_license file [<i>license</i>]
Displays the license in use.	show license usage
Displays the serial number of the device where the license is installed.	show license hostid
Displays the unbound license code on the current device.	show license unbind-code

10. CONFIGURING MODULE HOT SWAPPING

10.1. Overview

Module Hot Swapping is a common maintenance function provided by chassis-based devices.

Module Hot Swapping automates the installation, uninstallation, reset, and information check of hot-swappable modules (management cards, line cards, cross-connect and synchronous timing boards [XCSs], and multi-service cards) after they are inserted into chassis-based devices.

10.2. Applications

Application	Description
Resetting Online Modules	During routine maintenance, you can reset an abnormally running module to troubleshoot the fault.
Clearing the Configuration of a Module	During routine maintenance, you can replace the module in a slot with a different type of module.
Clearing the Configuration of a Virtual Switch Unit (VSU) Member Device	During routine maintenance, you can clear the configuration of all modules on a VSU member device and then reconfigure the modules.
Deleting a MAC Address from the Configuration File	During routine maintenance, you can delete the MAC addresses of VSU member devices to perform MAC address reelection.
Modifying a MAC Address in the Configuration File	When you replace a switch with a new one in gateway mode, you can configure the MAC address of the new switch to be the same as that of the replaced switch to retain the MAC address of the bound gateway on downstream devices.

10.2.1. Resetting Online Modules

Scenario

During routine maintenance, you can reset an abnormally running module in a slot to troubleshoot the fault.

Deployment

Run the **reset module** command on the console to reset a module.

10.2.2. Clearing the Configuration of a Module

Scenario

During routine maintenance, you can replace the module in a slot on a chassis-based device with a different type of module without affecting other modules.

Deployment

Perform the following operations in sequence:

1. Remove the module from the target slot.
2. Run the **remove configuration module** command on the device to remove the module configuration.
3. Insert a new module into the slot.

10.2.3. Clearing the Configuration of a VSU Member Device

Scenario

In VSU mode, to meet service change requirements, you need to clear all configurations on a member device and reconfigure the device. You can run the **remove configuration device** command to clear configurations all at once, rather than clear the configuration of individual modules one by one on the member device.

Deployment

Perform the following operations in sequence:

1. Run the **remove configuration device** command on the target device.
2. Save the configuration.
3. Restart the VSU and check whether the configuration of the device is cleared.

10.2.4. Deleting the MAC Address from the Configuration File

Scenario

In general, the MAC address used by a system is written in the management card or the flash memory of the chassis. In VSU mode, to avoid service interruption due to the change of the MAC address, the system automatically saves the MAC address to the configuration file. After the system restarts, the valid MAC address (if any) in the configuration file is used in preference. The **no sysmac** command can be used to delete the MAC address from the configuration file. Then the MAC address written in the flash memory is used by default.

Deployment

Perform the following operations in sequence:

1. Run the **no sysmac** command on the target device to delete its MAC address.
2. Save the configuration.
3. Restart the VSU and check whether the MAC address of the device is reelected.

10.2.5. Modifying a MAC Address in the Configuration File

Scenario

In gateway mode (the **auth-mode gateway** command is configured), some peripheral devices are configured with the MAC address of the bound gateway. If the gateway is replaced, you can use the **sysmac** command to configure the MAC address of the new gateway to be the same as that of the replaced gateway to retain the MAC address of the bound gateway on downstream devices. The **sysmac** command is valid only in gateway mode.

Deployment

Perform the following operations in sequence:

1. Run the **sysmac** command in gateway mode on the target device.
2. Save the configuration.
3. Restart the device and check whether its MAC address is modified.

10.3. Features

Feature

Feature	Description
<u>Automatically Installing the Inserted Module</u>	After a new module is inserted into a chassis-based device, the device's management software will automatically install the module driver.
<u>Resetting Online Modules</u>	Online modules can be reset.

10.3.1. Automatically Installing the Inserted Module

You can hot-swap (insert and remove) a module on a device in running state without impact on other modules. After the module is inserted into a slot, the device's management software will automatically install the module driver. The configuration of the removed module is retained for subsequent configuration. If the removed module is inserted again, the module will be automatically started with its configuration effective.

↪ The module mentioned here can be a management card, a line card, an XCS, or a multi-service card. A management card can only be inserted in a management card slot (M1 or M2). A line card or multi-service card can be inserted in a line card slot. An XCS can only be inserted in an XCS slot.

Working Principle

After a module is inserted, the device's management software will automatically install the module driver and save the module information (such as the quantity of ports on the module and port type) to the device, which will be used for subsequent configuration. After the module is removed, its information is not cleared by the management software. You can continue to configure the module information. When the module is inserted again, the management software assigns the user's module configuration to the module and make it take effect.

10.3.2. Resetting Online Modules

The management software of a device provides the online module reset feature for module software troubleshooting.

⚠ Resetting an online module may interrupt some services on the device.

Working Principle

After you run the **reset module** command, the device's management software uses a hardware or software interface of the device to restart the software on the target module and restores the hardware chip to the post-power-on state. The software failure of the module will be rectified after the module is reset.

10.4. Configuration

⚠ The module Hot Swapping feature is automatically implemented without manual configuration.

Configuration	Description and Command	
<u>Clearing Module and Device Configuration</u>	⚠ (Optional) It is used to clear configuration in global configuration mode. After you run the following commands, you need to save the command configuration so that it can take effect after system restart.	
	remove configuration module [<i>device-id</i>] <i>slot-num</i>	Clears the configuration of a module.
	remove configuration device <i>device-id</i>	Clears the configuration of a VSU member device.
	no sysmac	Deletes a MAC address from the configuration file.

10.4.1. Clearing Module and Device Configuration

Configuration Effect

- Clear the configuration of a module.

- Clear the configuration of a VSU member device.
- Delete a MAC address from the configuration file.

Configuration Steps

→ Clearing the Configuration of a Module

- (Optional) Perform this configuration when you need to remove a card from a slot on a device and delete related port configuration.

Command	remove configuration module [<i>device-id</i>]/ <i>slot-num</i>
Parameter Description	<i>device-id</i> : Indicates the ID of a chassis (in VSU mode, you must input the ID of the chassis housing the module to be removed. In stand-alone, the input is not required). <i>slot-num</i> : Indicates the number of the slot for the module.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to clear the configuration of a module (or a board not in position). ⚠ This command is forbidden for online cards to prevent the anti-loop configuration on online cards from being cleared causing network loops.

→ Clearing the Configuration of a VSU Member Device

- (Optional) Perform this configuration when you need to clear the configuration of a VSU member device.

Command	remove configuration device <i>device-id</i>
Parameter Description	<i>device-id</i> : Indicates the ID of a chassis.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to clear the configuration of a VSU member device.

→ Deleting a MAC Address from the Configuration File

- (Optional) Perform this configuration when you need to change the MAC address of a system to the reelected MAC address.
- In general, the MAC address used by a system is written in the management card or the flash memory of the chassis. In VSU mode, to avoid service interruption due to the change of the MAC address, the system automatically saves the MAC address to the configuration file. After the system restarts, the valid MAC address (if any) in the configuration file is used in preference.

Command	no sysmac
Parameter Description	N/A
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to delete a MAC address from the configuration file. Then the MAC address written in the flash memory is used by default.

→ Modifying a MAC Address in the Configuration File

- (Optional) Perform this configuration when you need to modify the MAC address of a device.
- In gateway mode (the **auth-mode gateway** command is configured), some peripheral devices are configured with the MAC address of the bound gateway. If the gateway is replaced, you can use the **sysmac** command to configure the MAC address of the new gateway to be the same as that of the replaced gateway to retain the MAC address of the bound gateway on downstream devices. The **sysmac** command is valid only in gateway mode.

Command	sysmac <i>mac-address</i>
Parameter Description	<i>mac-address</i> : Indicates the new MAC address.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to configure the MAC address of a device. To make the MAC address take effect, save the configuration and restart the device.

Verification

Run the **show version slot** command to display the installation information of a line card.

Command	show version slots [<i>device-id / slot-num</i>]
Parameter Description	<i>device-id</i> : (Optional) Indicates the ID of a chassis (in VSU mode, when you input a slot number, you also need to input the ID of the chassis where the module is located). <i>slot-num</i> : (Optional) Indicates the number of a slot.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to display the online state of a module. The Configured Module column shows the information of the installed module. After you run the remove configuration module command, the installation information of the removed module is deleted from this column.


```

Show the module online status information
QTECH# show version slots
Dev Slot Port Configured Module Online Module
Software Status
-----
1 1 0 none none none
1 2 52 QSW-M7600-48GT4XS-EB QSW-M7600-48GT4XS-EB
ok
1 6 0 none none none
1 M1 0 N/A QSW-M7608-CM
master
1 M2 0 N/A none none

```

Configuration Example

→ Clearing the Configuration of an Offline Module

Scenario	<ul style="list-style-type: none"> To meet networking change requirements, the port configuration of the card in Slot 1 needs to be deleted to make the device's configuration file more concise.
Configuration Steps	<ul style="list-style-type: none"> Run the remove configuration module command to delete the card configuration.
	<pre>QTECH(config)# remove configuration module 1</pre>
	<pre> Run the show version slots command to verify that the card configuration in Slot 1 is cleared. QTECH# show version slots Dev Slot Port Configured Module Online Module Software Status ----- 1 1 0 none none none 1 2 52 QSW-M7600-48GT4XS-EB QSW-M7600-48GT4XS-EB ok 1 6 0 none none none 1 M1 0 N/A QSW-M7608-CM master 1 M2 0 N/A none none </pre>

10.5. Monitoring

Clearing

👉 Running the reset module command may interrupt services when the module is reset.

Description	Command
Resets a module	reset module <i>slot-num</i> reset module <i>device-id / slot-num</i> (in VSU mode)

Displaying

Description	Command
Displays the details of a module.	show version module detail [<i>slot-num</i>] show version module detail [<i>device-id/slot-num</i>] (in VSU mode)
Displays the online state of a module.	show version slots [<i>slot-num</i>] show version slots [<i>device-id/slot-num</i>] (in VSU mode)

11. CONFIGURING SUPERVISOR MODULE REDUNDANCY

11.1. Overview

Supervisor module redundancy is a mechanism that adopts real-time backup (also called hot backup) of the service running status of supervisor modules to improve the device availability.

In a network device with the control plane separated from the forwarding plane, the control plane runs on a supervisor module and the forwarding plane runs on cards. The control plane information of the master supervisor module is backed up to the slave supervisor module in real time during device running. When the master supervisor module is shut down as expected (for example, due to software upgrade) or unexpectedly (for example, due to software or hardware exception), the device can automatically and rapidly switch to the slave supervisor module without losing user configuration, thereby ensuring the normal operation of the network. The forwarding plane continues with packet forwarding during switching. The forwarding is not stopped and no topology fluctuation occurs during the restart of the control plane.

The supervisor module redundancy technology provides the following conveniences for network services:

- Improving the network availability

The supervisor module redundancy technology sustains data forwarding and the status information about user sessions during switching.

- Preventing neighbors from detecting link flaps

The forwarding plane is not restarted during switching. Therefore, neighbors cannot detect the status change of a link from Down to Up.

- Preventing route flaps

The forwarding plane sustains forwarding communication during switching, and the control plane rapidly constructs a new forwarding table. The process of replacing the old forwarding table with the new one is unobvious, preventing route flaps.

- Preventing loss of user sessions

Thanks to real-time status synchronization, user sessions that are created prior to switching are not lost.

11.2. Applications

Application	Description
-------------	-------------

Redundancy of Supervisor Modules

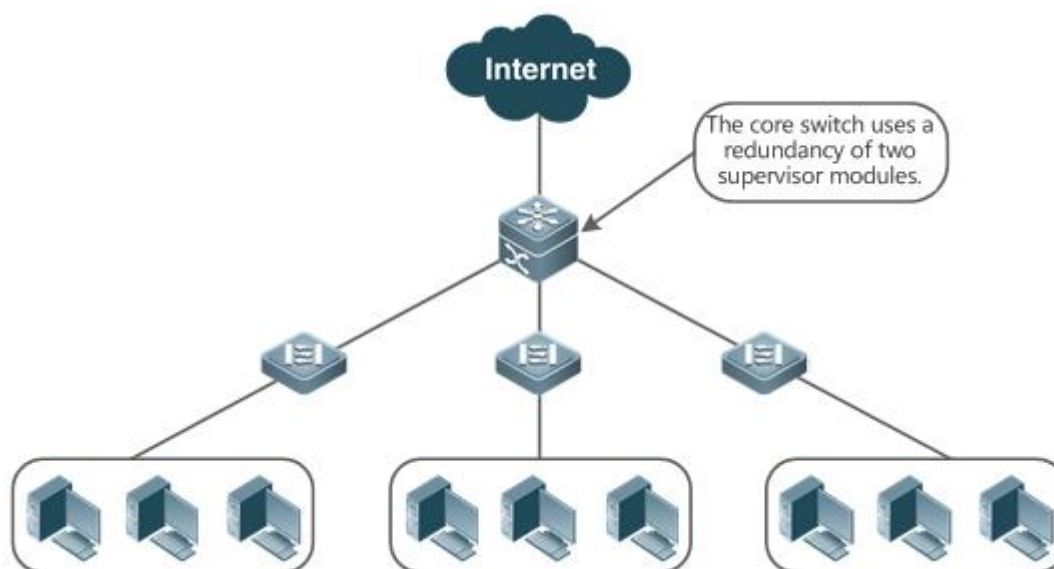
On a core switch where two supervisor modules are installed, the redundancy technology can improve the network stability and system availability.

11.2.1. Redundancy of Supervisor Modules

Scenario

As shown in the following figure, in this network topology, if the core switch malfunctions, networks connected to the core switch break down. In order to improve the network stability, two supervisor modules need to be configured on the core switch to implement redundancy. The master supervisor module manages the entire system and the slave supervisor module backs up information about service running status of the master supervisor module in real time. When manual switching is performed or forcible switching is performed due to a failure occurring on the master supervisor module, the slave supervisor module immediately takes over functions of the master supervisor module. The forwarding plane can proceed with data forwarding and the system availability is enhanced.

Figure 11-1



Deployment

For chassis-type devices, the system is equipped with the master/slave backup mechanism. The system supports plug-and-play as long as master and slave supervisor modules conform to redundancy conditions.

For case-type devices, each device is equivalent to one supervisor module and one line card. The virtual switching unit (VSU) composed of multiple case-type devices also has the master/slave backup mechanism.

11.3. Features

Basic Concepts

→ Master Supervisor Module, Slave Supervisor Module

On a device where two supervisor modules are installed, the system elects one supervisor module as active, which is called the master supervisor module. The other supervisor module functions as a backup supervisor module. When the master supervisor module malfunctions or actively requests switching, the backup supervisor module takes over the functions of the master supervisor module and becomes the new master supervisor module, which is called the slave supervisor module. In general, the slave supervisor module does not participate in switch management but monitors the running status of the master supervisor module.

→ Globally Master Supervisor Module, Globally Slave Supervisor Module, Globally Candidate Supervisor Module

In a VSU system composed of two or more chassis-type devices, each chassis has two supervisor modules, with the master supervisor module managing the entire chassis and the slave supervisor module functioning as a backup. For the entire VSU system, there are two or more supervisor modules. One master supervisor module is elected out of the supervisor modules to manage the entire VSU system, one slave supervisor module is elected as the backup of the VSU system, and other supervisor modules are used as candidate supervisor modules. A candidate supervisor module replaces the master or slave supervisor module and runs as the master or slave supervisor module when the original master or slave supervisor module malfunctions. In general, candidate supervisor modules do not participate in backup. To differentiate master and slave supervisor modules in a chassis from those in a VSU system, the master, slave, and candidate supervisor modules in a VSU system are called "globally master supervisor module", "globally slave supervisor module," and "globally candidate supervisor module" respectively. The redundancy mechanism of supervisor modules takes effect on the globally master supervisor module and globally slave supervisor module. Therefore, the master and slave supervisor modules in the VSU environment are the globally master supervisor module and globally slave supervisor module.

In a VSU system composed of two or more case-type devices, each case-type device is equivalent to one supervisor module and one line card. The system elects one device as the globally master supervisor module and one device as the globally slave supervisor module, and other devices serve as globally candidate supervisor modules.

→ Prerequisites for Redundancy of Supervisor Modules

In a device system, the hardware and software of all supervisor modules must be compatible so that the redundancy of supervisor modules functions properly.

Batch synchronization is required between the master and slave supervisor modules during startup so that the two supervisor modules are in the same state. The redundancy of supervisor modules is ineffective prior to synchronization.

→ Redundancy Status of Supervisor Modules

The master supervisor module experiences the following status changes during master/slave backup:

- alone state: In this state, only one supervisor module is running in the system, or the master/slave switching is not complete, and redundancy is not established between the new master supervisor module and the new slave supervisor module.
- batch state: In this state, redundancy is established between the master and slave supervisor modules and batch backup is being performed.
- realtime state: The master supervisor module enters this state after the batch backup between the master and slave supervisor modules is complete. Real-time backup is performed between the master and slave supervisor modules, and manual switching can be performed only in this state.

Overview

Feature	Description
<u>Election of Master and Slave Supervisor Modules</u>	The device can automatically select the master and slave supervisor modules based on the current status of the system. Manual selection is also supported.
<u>Information Synchronization of Supervisor Modules</u>	In the redundancy environment of supervisor modules, the master supervisor module synchronizes status information and configuration files to the slave supervisor module in real time.

11.3.1. Election of Master and Slave Supervisor Modules

Working Principle

→ Automatically Selecting Master and Slave Supervisor Modules for Chassis-type Devices

Users are allowed to insert or remove supervisor modules during device running. The device, based on the current condition of the system, automatically selects an engine for running, without affecting the normal data switching. The following cases may occur and the master supervisor module is selected accordingly:

- If only one supervisor module is inserted during device startup, the device selects this supervisor module as the master supervisor module regardless of whether it is inserted into the M1 slot or M2 slot.
- If two supervisor modules are inserted during device startup, by default, the supervisor module in the M1 slot is selected as the master supervisor module and the supervisor module in the M2 slot is selected as the slave supervisor module to serve as a backup, and relevant prompts are output.
- If one supervisor module is inserted during device startup and another supervisor module is inserted during device running, the supervisor module that is inserted later is used as the slave supervisor module to serve as a backup regardless of whether it is inserted into the M1 slot or M2 slot, and relevant prompts are output.
- Assume that two supervisor modules are inserted during device startup and one supervisor module is removed during device running (or one supervisor module malfunctions). If the removed supervisor module is the slave supervisor module prior to removal (or failure), only a prompt is displayed after removal (or malfunction), indicating that the slave supervisor module is removed (or fails to run). If the removed supervisor module is the master supervisor module prior to removal (or failure), the other supervisor module becomes the master supervisor module and relevant prompts are output.

→ Manually Selecting the Master and Slave Supervisor Modules

Users can manually make configuration to select the master and slave supervisor modules, which are selected based on the environment as follows:

- In standalone mode, users can manually perform master/slave switching. The supervisor modules take effect after reset.
- In VSU mode, users can manually perform master/slave switching to make the globally slave supervisor module become the globally master supervisor module. If a VSU system has only two supervisor modules, the original globally master supervisor module becomes the new globally slave supervisor module after reset. If there are more than two supervisor modules, one globally candidate supervisor module is elected as the new globally slave supervisor module and the original globally master supervisor module becomes a globally candidate supervisor module after reset.

Related Configuration

→ Manually Performing Master/Slave Switching

- By default, the device can automatically select the master supervisor module.
- In both the standalone and VSU modes, users can run the `redundancy forceswitch` command to perform manual switching.

11.3.2. Information Synchronization of Supervisor Modules

Working Principle

- Status synchronization

The master supervisor module synchronizes its running status to the slave supervisor module in real time so that the slave supervisor module can take over the functions of the master supervisor module at any time, without causing any perceivable changes.

- Configuration synchronization

There are two system configuration files during device running: running-config and startup-config. running-config is a system configuration file dynamically generated during running and changes with the service configuration. startup-config is a system configuration file imported during device startup. You can run the write command to write running-config into startup-config or run the copy command to perform the copy operation.

For some functions that are not directly related to non-stop forwarding, the synchronization of system configuration files can ensure consistent user configuration during switching.

In the case of redundancy of dual supervisor modules, the master supervisor module periodically synchronizes the startup-config and running-config files to the slave supervisor module and all candidate supervisor modules. The configuration synchronization is also triggered in the following operations:

- The running-config file is synchronized when the device switches from the global configuration mode to privileged EXEC mode.
- The startup-config file is synchronized when the **write** or **copy** command is executed to save the configuration.
- Information configured over the Simple Network Management Protocol (SNMP) is not automatically synchronized and the synchronization of the running-config file needs to be triggered by running commands on the CLI.

Related Configuration

- By default, the startup-config and running-config files are automatically synchronized once per hour.
- Run the **auto-sync time-period** command to adjust the interval for the master supervisor module to synchronize configuration files.

11.4. Configuration

Configuration	Description and Command
---------------	-------------------------

Configuring Manual Master/Slave Switching	Optional.	
	show redundancy states	Displays the hot backup status.
	redundancy forceswitch	Manually performs master/slave switching.
Configuring the Automatic Synchronization Interval	Optional.	
	redundancy	Enters the redundancy configuration mode.
	auto-sync time-period	Configures the automatic synchronization interval of configuration files in the case of redundancy of dual supervisor modules.
Resetting Supervisor Modules	Optional.	
	redundancy reload	Resets the slave supervisor module or resets both the master and slave supervisor modules at the same time.

11.4.1. Configuring Manual Master/Slave Switching

Configuration Effect

The original master supervisor module is reset and the slave supervisor module becomes the new master supervisor module.

If there are more than two supervisor modules in the system, the original slave supervisor module becomes the master supervisor module, one supervisor module is elected out of candidate supervisor modules to serve as the new slave supervisor module, and the original master supervisor module becomes a candidate supervisor module after reset.

Notes

To ensure that data forwarding is not affected during switching, batch synchronization needs to be first performed between the master and slave supervisor modules so that the two supervisor modules are in the same state. That is, manual switching can be performed only when the redundancy of supervisor modules is in the real-time backup state. In addition, to ensure synchronization completeness of configuration files, service modules temporarily forbid manual master/slave switching during synchronization. Therefore, the following conditions need to be met simultaneously for manual switching:

- Manual master/slave switching is performed on the master supervisor module and a slave supervisor module is available.
- All virtual switching devices (VSDs) in the system are in the real-time hot backup state.

- The hot-backup switching of all VSDs in the system is not temporarily forbidden by service modules.

If devices are virtualized as multiple VSDs, manual switching can be successfully performed only when the supervisor modules of all the VSDs are in the real-time backup state.

Configuration Steps

- Optional.
- Make the configuration on the master supervisor module.

Verification

Run the **show redundancy states** command to check whether the master and slave supervisor modules are switched.

Related Commands

→ Checking the Hot Backup Status

Command	show redundancy states
Parameter Description	N/A
Command Mode	Privileged EXEC mode or global configuration mode
Usage Guide	N/A

→ Manually Performing Master/Slave Switching

Command	redundancy forceswitch
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuration Example

→ Manually Performing Master/Slave Switching

Configuration Steps	In the VSD environment where the name of one VSD is staff, perform master/slave switching.
	<pre>QTECH> enable QTECH# show redundancy states Redundancy role: master</pre>

	<pre>Redundancy state: realtime Auto-sync time-period: 3600 s VSD staff redundancy state: realtime QTECH# redundancy forceswitch This operation will reload the master unit and force switchover to the slave unit. Are you sure to continue? [N/y] y</pre>
Verification	On the original slave supervisor module, run the show redundancy states command to check the redundancy status.
	<pre>QTECH# show redundancy states Redundancy role: master Redundancy state: realtime Auto-sync time-period: 3600 s VSD staff redundancy state: realtime</pre>

11.4.2. Configuring the Automatic Synchronization Interval

Configuration Effect

Change the automatic synchronization interval of the startup-config and running-config files. If the automatic synchronization interval is set to a smaller value, changed configuration is frequently synchronized to other supervisor modules, preventing the configuration loss incurred when services and data are forcibly switched to the slave supervisor module when the master supervisor module malfunctions.

Configuration Steps

- Optional. Make the configuration when the synchronization interval needs to be changed.
- Make the configuration on the master supervisor module.

Verification

- View the output syslogs to check whether timed synchronization is performed.

Related Commands

→ Entering the Redundancy Configuration Mode

Command	redundancy
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

→ Configuring the Automatic Synchronization Interval of Configuration Files

Command	Auto-sync time-period <i>value</i>
Parameter Description	time-period <i>value</i> : Indicates the automatic synchronization interval, with the unit of seconds. The value ranges from 1 second to 1 month (2,678,400 seconds).
Command Mode	Redundancy configuration mode
Usage Guide	Configure the automatic synchronization interval of the startup-config and running-config files in the case of redundancy of dual supervisor modules.

Configuration Example

→ Configuring the Automatic Synchronization Interval

Configuration Steps	In redundancy configuration mode of the master supervisor module, configure the automatic synchronization interval to 60 seconds.
	<pre>QTECH(config)# redundancy QTECH(config-red)# auto-sync time-period 60 Redundancy auto-sync time-period: enabled (60 seconds). QTECH(config-red)# exit</pre>
Verification	Run the show redundancy states command to check the configuration.
	<pre>QTECH# show redundancy states Redundancy role: master Redundancy state: realtime Auto-sync time-period: 3600 s</pre>

11.4.3. Resetting Supervisor Modules

Configuration Effect

Resetting only the slave supervisor module does not affect data forwarding, and the forwarding is not interrupted or user session information is not lost during reset of the slave supervisor module.

In standalone mode, running the **redundancy reload shelf** command will cause simultaneous reset of all supervisor modules and line cards in the chassis. In VSU mode, the device of a specified ID is reset when this command is executed. If there are two or more devices in the system and the device to be reset is the device where the globally master supervisor module resides, the system performs master/slave switching.

Notes

In VSU mode, if the supervisor modules of the system do not enter the real-time backup state, resetting the device where the globally master supervisor module resides will cause the reset of the entire VSU system.

Configuration Steps

- Optional. Perform the reset when the supervisor modules or device runs abnormally.

Related Commands

Command	redundancy reload {peer shelf [switchid]}
Parameter Description	peer: Only resets the slave supervisor module. shelf [switchid]: Indicates that the master and slave supervisor modules are set in standalone mode, and the ID of the device to be reset needs to be specified in VSU mode.
Command Mode	Privileged EXEC mode
Usage Guide	In standalone mode, the device reset command is redundancy reload shelf , that is, the entire device is reset. In VSU mode, the device reset command is redundancy reload shelf switchid , that is, the device of a specified device ID is reset.

Configuration Example

→ Resetting a Device in VSU Mode

Configuration Steps	In privileged EXEC mode of the globally master supervisor module, reset the device with the ID of 2.
	<pre>QTECH# redundancy reload shelf 2 This operation will reload the device 2. Are you sure to continue? [N/y] y Preparing to reload device 2!</pre>
Verification	Check whether the relevant supervisor module or device is restarted.

11.5. Monitoring

Displaying

Description	Command
Displays the current redundancy status of dual supervisor modules.	show redundancy states

12. CONFIGURING USB

12.1. Overview

Universal serial bus (USB) is an external bus standard. In this document, USB refers to a USB-compliant peripheral device, for example, a USB flash drive.

USB is a hot swappable device. You can use it to copy files (such as configuration and log files) from a communication device, or copy external data (such as system upgrade files) to the flash of the communication device.

Specific application scenarios of the USB are detailed in configuration guides of related functions. This document describes only how to identify, use, and remove the USB and view information about the USB.

12.2. Applications

Application	Description
Using a USB Flash Drive to Upgrade a Device	Upgrade files are stored on a USB flash drive. After a device is powered on, the device detects the USB flash drive and runs the upgrade command to load the upgrade files. After loading is completed, the device is reset and runs the upgraded version.

12.2.1. Using a USB Flash Drive to Upgrade a Device

Scenario

Upgrade files are stored on a USB flash drive. After a device is powered on, the device detects the USB flash drive and runs the upgrade command to load the upgrade files. After loading is completed, the device is reset and runs the upgraded version. An example of the upgrade command is as follows:

```
upgrade usb0:/s12k-ppc_11.0(1B2)_20131025_main_install.bin
```

If the file is valid and execution of this command succeeds, the device will be automatically reset and run the upgraded version.

Deployment

- Use the prefix "usb0:/" to access USB 0. Run the **show usb** command to display information about the USB with the ID 0.
- Run the **upgrade** command to perform upgrade.

12.3. Features

→ Using the USB

Insert a USB into the USB slot. The system automatically searches for the USB. After the USB is located, the driver module automatically initializes the driver of the USB. After initialization, the system automatically loads the file system on the USB. Later, the system can read or write this USB.

- If the system finds a USB and successfully loads the driver, the following information will be displayed:

```
*Jan 1 00:09:42: %USB-5-USB_DISK_FOUND: USB Disk <Mass Storage> has been inserted
to USB port 0!

*Jan 1 00:09:42: %USB-5-USB_DISK_PARTITION_MOUNT: Mount usb0 (type:FAT32), size :
1050673152B (1002MB)
```

↪ "Mass Storage" indicates the name of the searched device, and "usb0:" indicates the first USB. "Size" indicates the size of the partition. For example, according to the preceding information displayed, the USB flash drive has a space of 1002 MB.

→ Removing the USB

Use a command line interface (CLI) command to remove the USB first; otherwise, an error may occur if the system is currently using the USB.

- If the USB is successfully removed, the following information will be displayed:

```
OK, now you can pull out the device 0.
```

You can remove the USB only after the preceding information is displayed.

12.4. Configuration

Configuration	Description and Command
Using a USB	👉 Mandatory.
	N/A
Removing a USB	👉 (Mandatory) It is used to remove a USB.
	<code>usb remove</code> Removes a USB.

12.4.1. Using a USB

Configuration Effect

After a USB is loaded, you can run the file system commands (such as `dir`, `copy`, and `del`) to perform operations on the USB.

Notes

- The QTECH General Operating System is applicable only to devices (generally common USB flash drives) that support standard Small Computer System Interface (SCSI) commands. Other devices, such as the USB flash drive embedded in the USB network interface card (NIC) and USB flash drive with the virtual CD-ROM drive, cannot be used in the RGOS. Some devices are configured with the function of converting a USB port to the serial port.
- The USB supports only the FAT file system. Other file systems on the USB must be formatted to the FAT file system on a PC before the USB can be used on a device.
- The RGOS supports the hub. When a USB flash drive is inserted to a port on a hub, the access path becomes different. If the USB flash drive is inserted to a USB port on a device, the access path is **usbX:/**, where **X** indicates the device ID. You can run the **show usb** command to display this path. If the USB flash drive is inserted to a USB port through a hub, the access path is **usbX-Y:/**, where **X** indicates the device ID, and **Y** indicates the hub port ID. For example, **usb0-3:/** indicates port 3 on the hub that is connected to USB port 0 on the device.

Configuration Steps

→ Identifying a USB

A USB can be directly inserted to the USB slot without a CLI operation.

→ Using a USB

Perform the following operations to copy files from a USB to the flash:

- Run the **cd** command to enter the partition of the USB.
- Run the **copy** command to copy files on the USB to the flash on the device.
- Run the **dir** command to check whether the files are copied to the device.

⚠ If the USB has multiple partitions, you can access only the first FAT partition on the device.

⚠ The path of the USB does not contain any upper-level directory. After running the **cd usbX:** command to access a USB, you can run the **cd flash:** command to return to the flash file system.

Verification

Run the **show usb** command to display information about the USB inserted to the device.

Configuration Example

→ Using a USB Flash Drive

Scenario	Standalone environment
Configuration Steps	<ul style="list-style-type: none"> • Insert the USB flash drive into the USB slot of the device.

	<ul style="list-style-type: none">● Run the show usb command on the device console.● Copy the config.txt file from the USB flash drive to the flash on the device.
	<pre>QTECH#show usb Device: Mass Storage ID: 0 URL prefix: usb0 Disk Partitions: usb0 (type:vfat) Size:15789711360B(15789.7MB) Available size:15789686784B(15789.6MB) QTECH# QTECH# QTECH#dir usb0:/ Directory of usb0:/ 1 -rwx 4 Tue Jan 1 00:00:00 1980 fac_test 2 -rwx 1 Mon Sep 30 13:15:48 2013 config.txt 2 files, 0 directories 15,789,711,360 bytes total (15,789,686,784 bytes free) QTECH# QTECH# QTECH#copy usb0:/config.txt flash:/ Copying: ! Accessing usb0:/config.txt finished, 1 bytes prepared Flushing data to flash:/config.txt... Flush data done QTECH# QTECH#</pre>
Verification	<ul style="list-style-type: none">● Check whether the config.txt file exists on the flash.
	<pre>QTECH# QTECH#dir flash:/ Directory of flash:/ 1 drw- 160 Wed Mar 31 08:40:01 2010 at 2 drwx 160 Thu Jan 1 00:00:11 1970 dm 3 drwx 160 Thu Jan 1 00:00:05 1970 rep 4 drwx 160 Mon Apr 26 03:42:00 2010 scc</pre>

```
5 drwx      160 Wed Mar 31 08:39:52 2010  ssh
6 drwx      224 Thu Jan  1 00:00:06 1970  var
7 d---      288 Sat May 29 06:07:45 2010  web
8 drwx      160 Thu Jan  1 00:00:11 1970  addr
9 drwx      160 Sat May 29 06:07:44 2010  cwmp
10 drwx     784 Sat May 29 06:07:47 2010  sync
11 --w-      92 Tue Feb  2 01:06:55 2010  config_vsu.dat
12 -rw-     244 Sat Apr  3 04:56:52 2010  config.text
13 -rwx        1 Thu Jan  1 00:00:30 1970  .issu_state
14 -rw-        0 Tue Feb  2 01:07:03 2010  ss_ds_debug.txt
15 -rw-    8448 Thu Jan  1 00:01:41 1970  .shadow
16 -rwx     268 Thu Jan  1 00:01:41 1970  .pswdinfo
17 -rw-        4 Tue May 25 09:12:01 2010  reload
18 drwx     232 Wed Mar 31 08:40:00 2010  snpv4
19 drwx    6104 Sat May 29 06:10:45 2010  .config
20 ----        1 Thu Jan  1 00:04:51 1970  config.txt
21 d---     160 Thu Jan  1 00:00:12 1970  syslog
22 drwx     160 Tue May 25 03:05:01 2010  upgrade_ram
23 drwx     160 Tue Feb  2 01:06:54 2010  dm_vdu
24 -rwx     16  Thu Jan  1 00:01:41 1970  .username.data

9 files, 15 directories
5,095,424 bytes total (4,960,256 bytes free)
QTECH#
```

Common Errors

- Insert a USB flash drive that supports non-SCSI commands to the device.
- The USB does not use the FAT file system, and cannot be identified by the system.

12.4.2. Removing a USB

Configuration Effect

Remove the USB and ensure that the USB and the device are intact.

Notes

- Run the **usb remove** command before removing the USB; otherwise, a system error occurs.

Configuration Steps

→ Running the Remove Command

- Mandatory.

- Run the **usb remove** or **sd remove** command before removing the USB.

Removing the USB

After the remove command is executed, remove the USB.

Verification

Run the **show usb** command to display information about the USB inserted to the device.

Related Commands

→ Removing a USB

Command	usb remove <i>device-id</i>
Parameter Description	<i>device-id</i> : Indicates the ID of the USB port on the device. You can run the show usb command to display this ID.
Command Mode	Privileged EXEC mode
Usage Guide	Before removing a USB, run the usb remove command; otherwise, an error occurs if the USB is in use. If the command is executed, related information will be displayed, and you can remove the USB. If the command execution fails, the USB is in use. In this case, do not remove the USB until it is not in use.

Configuration Example

→ Removing a USB

Scenario	Standalone environment
Configuration Steps	<ul style="list-style-type: none"> ● Run the show usb command to display the ID of the USB. ● Run the usb remove command to remove the USB.
	<pre> QTECH#show usb Device: Mass Storage ID: 0 URL prefix: usb0 Disk Partitions: usb0 (type:vfat) Size:15789711360B (15789.7MB) Available size:15789686784B (15789.6MB) QTECH# QTECH# QTECH#usb remove 0 OK, now you can pull out the device 0. </pre>

Verification	<ul style="list-style-type: none">• Run the show usb command again to check whether the USB is removed. If the device with ID 0 is not displayed in output of the show usb command, the USB is removed.
	<pre>QTECH#show usb QTECH#</pre>

12.5. Monitoring

Displaying

Description	Command
Displays information about the inserted USB.	show usb

13. CONFIGURING POE

13.1. Overview

Power over Ethernet (PoE) is a technology that can transmit electricity and data to devices through twisted pairs over Ethernet. This technology enables various devices such as VOIP, WIFI APs, network cameras, hubs and computers to obtain electricity through twisted pairs.

The largest distance that can be powered by a PoE switch is 100 m as defined by the standards. A PoE switch can collect statistics about the power supplies of all ports and the entire device, which can be displayed by a query command.

Protocols and Standards

Currently, PoE complies with the IEEE 802.3af and IEEE 802.3at standards. The following table lists the main characteristics of and differences between the two standards:

Parameter	802.3af	802.3at
Available Power for PD	12.95 W	25.50 W
Maximum Power Provided by PSE	15.4 W	30 W
Voltage Range of PSE	44.0-57.0 V	50.0-57.0 V
Voltage Range of PD	37.0-57.0 V	42.5-57.0 V
Maximum Resistance of Network Cables	20 Ω	12.5 Ω
Power Management Mode	Classify power levels during line initialization.	Classify the power supply into 4 levels during line initialization or dynamically adjust the power supply in the unit of 0.1 W.
Supported Cables	Cat-3 or Cat-5 twisted pairs	Cat-5 twisted pairs

13.2. Applications

Application	Description
<u>PoE Power Supply Scenario</u>	In the scenario, a PoE switch powers powered devices (PDs) and implements data exchange.

13.2.1. PoE Power Supply Scenario

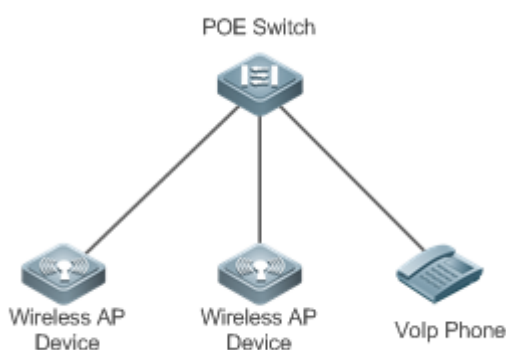
Scenario

In a PoE system set up with a PoE switch, the PoE switch combines the PoE power supply with the PSE. In addition to providing normal network data exchange, the PoE switch also provides the power supply function. The main PDs in the system include the APs of a WLAN and VoIP telephones.

The PoE switch provides power management, including power supply enabling for ports, power supply priority management, over-temperature protection for ports, and power supply status query for devices and ports.

A PoE switch enabling PoE+ supports LLDP correlation with PDs for dynamically managing the power supply power of ports.

Figure 13-1



Deployment

- By default, a PoE switch port is enabled with the power supply function and can start the power supply after detecting an accessed device.
- If the total power of the PoE system is insufficient, you can manually configure the power priority for ports to ensure that the ports are powered first.
- LLDP correlation is disabled by default. You can manually enable it as required.

13.3. Features

Basic Concepts

→ PoE Power Supply

The PoE power supply powers the entire PoE system and is classified into external and internal power supplies. Cassette PoE switches of QTECH often have internal power supplies and certain products also support external power supplies. External power supplies are called RPS.

→ PSE

Power Sourcing Equipment (PSE) queries and detects PDs on PoE ports, classifies PDs into different levels, and supplies power for the PDs. After detecting that a PD is removed, the PSE stops supplying power.

→ PD

PDs are devices powered by PSE and are classified into standard PDs and non-standard PDs. Standard PDs are PDs that comply with the IEEE 802.3af and 802.3at standards. Common non-standard PDs include non-standard PDs with featured resistance, Cisco pre-standard PDs, PDs supporting only signal cable power supplies, and PDs supporting only idle cable power supplies. QTECH switches use signal cable power supplies and do not support PDs supporting only idle cable power supplies.

When being powered by a PoE power supply, a PD can also connect to other power supplies for redundant backup of the power supplies.

Overview

Feature	Description
<u>Power Supply Management for PoE Line Cards</u>	Manages power supply enabling for PoE line cards and power allocation among line cards.
<u>Power Supply Management for the PoE System</u>	Manages the power supply policies of the system, such as the power supply mode and disconnection detection mode, and supports monitoring on the power supply of the PoE system, such as the system alarm limit and trap sending enabling/disabling.
<u>Power Supply Management for PoE Ports</u>	Manages the power supply policies of PoE ports, such as port enabling and power supply prioritization.
<u>Auxiliary PoE Power Supply Functions</u>	Provides auxiliary power supply management functions for the system, such as the power alarm limit of the system and PD descriptor configuration of ports.
<u>LLDP Classification</u>	PDs can dynamically adjust allocated power by exchanging LLDP packets with PSE.

13.3.1. Power Supply Management for PoE Line Cards

Working Principle

Power supply management for PoE line cards supports:

You can enable or disable the PoE function for line cards. If the PoE function is disabled for a line card, the line card will not be involved in power allocation.

You can set three priorities, namely, high, medium and low for line cards. The default priority is low. Line cards with high priorities can be allocated with power first and can preempt the power of line cards with low priorities. For line cards with the same priority, a smaller slot ID means a higher priority. Within the same priority, the power of line cards that have been powered on cannot be preempted.

You can configure allocated power for line cards.

Related Configuration

→ Enabling the Power Supply Function for Line Cards

- By default, line cards are enabled with the PoE power supply function.
- You can run the **no poe enable pse [device device_num] slot slot_num** command to disable the PoE function for a line card. Then, all PoE ports on the line card stop powering PDs.

→ Configuring Power Supply Priorities for Line Cards

By default, the priorities of line cards are low.

You can run the **poe priority { low | high | critical } pse [device device_num] slot slot_num** command to configure the power supply priority for a line card. If the power is insufficient, line cards with high priorities preempt the power of line cards with low priorities. In this case, certain ports of line cards with low priorities may be powered off due to insufficient power.

→ Configuring Allocated Power for Line Cards

By default, the power allocation for a line card is related to the number of PoE ports of the line card. The default power allocated to a line card with 24 PoE ports is 369.6 W and the default power allocated to a line card with 48 PoE ports is 739.2 W.

You can run the **poe max-power max-power pse [device device_num] slot slot_num** command to configure allocated power for a line card. If the total power required by all line cards is smaller than the system power, the system allocates power based on the user configuration; otherwise, the system allocates power based on priorities.

13.3.2. Power Supply Management for the PoE System

Working Principle

Power supply management for the PoE system supports:

You can switch the power supply mode (namely, the method for allocating power for PDs connected to the PoE switch). The PoE switch supports the auto mode and energy-saving mode for power supply management.

In the auto mode, the system allocates power based on the detected PD classes and types on ports. A PoE switch allocates power for PDs of classes 0 to 4 as follows: 15.4 W for Class0, 4

W for Class1, 7 W for Class2, 15.4 W for Class3, and 30 W for Class4. In this mode, even if there is a device of Class3 that consumes only 11 W, the PoE switch allocates a power of 15.4 W for the port connecting to this device. The auto mode is the default power supply management mode of the PoE switch.

In the energy-saving mode, the PoE switch dynamically adjusts allocated power based on actual consumption of PDs. In this mode, the PoE switch can power more PDs, but the power fluctuation of certain PDs may affect the power supply of other PDs. The energy-saving mode is an optional mode of the PoE switch. If the switch does not support this mode, corresponding prompt information will be displayed during configuration.

In the energy-saving mode, the PoE switch calculates the power consumption of the system based on the actual power consumption of the PDs. If certain PDs have a large power fluctuation in this mode, overload may occur on the PoE switch, which causes damage of the PoE device. The PoE switch provides a command for setting the reserved power of the PoE system to ensure that the PoE switch always has "rich" power and that the consumed power will not exceed the limit of the PoE switch.

The PoE switch identifies whether the PDs have been disconnected by using the disconnection detection function. In the DC disconnection detection mode (default), if the PoE switch detects that the port current is smaller than a specified value for a period, the PD connected to a port is considered as disconnected.

The PoE switch provides uninterruptible power supply during hot startup. When the system is restarted, PDs that are being powered will not be powered off during hot startup of the PoE switch. After the hot startup is completed, the system recovers the status saved in the configuration file.

Related Configuration

→ Configuring the Power Supply Management Mode

By default, the power supply management mode is auto.

You can run the **poe mode { auto | energy-saving }** command to configure the power supply management mode. Since different power management modes provide different methods for allocating power to PDs, mode switching may affect the PDs that can be powered.

→ Configuring the Reserved Power of the System

By default, the reserved power of the system is 0.

You can run the **poe reserve-power int** command to configure the reserved power of the system. When the system switches to the energy-saving mode, the reserved power configuration takes effect.

→ Configuring Uninterruptible Power Supply During Hot Startup

By default, the system disables the uninterruptible power supply function during hot startup.

You can run the **poe uninterruptible-power** command to enable the uninterruptible power supply function during hot startup. The configuration takes effect after being saved. During hot startup of the system, the PoE system supplies stable power for PDs.

13.3.3. Power Supply Management for PoE Ports

Working Principle

Power supply management for the PoE ports supports:

You can enable or disable the PoE function for ports.

You can configure power supply priorities for ports of a PoE switch. The priorities are Critical, High and Low in a descending order. In the auto and energy-saving modes, ports with high priorities are powered first. When the system power of the PoE switch is insufficient, ports with low priorities are powered off first. The default priorities of all ports are low.

Ports with the same priority are sorted by the port number. A smaller port number means a higher priority. For example, the priority of port 1 is higher than those of ports 2 and 3.

For ports with the same priority, newly inserted ports do not preempt the power of ports that are being powered. For ports with different priorities, ports with higher priorities can preempt the power of ports with lower priorities.

You can configure a switch to manage the power-on/off of a port based on time ranges. The time range can be configured by the time-range command in the global configuration mode.

You can configure the maximum power of a port to restrict the maximum output power of the port. In the auto and energy-saving modes, configuring the maximum power can restrict the maximum output power of ports. When the power of a port is greater than the configured maximum power for 10 seconds, the port is powered off, the device connected to the port is powered off, a log indicates power overload for the port, and the LED indicator of the port is displayed in yellow. 10 seconds later, the port is powered on again. If the power of the port is still greater than the maximum power for 10 seconds, the port will be powered off again. This process repeats constantly.

Currently, most PoE switches comply with the IEEE 802.3af and 802.3at standards in the industry. However, there are various PDs in actual applications, and certain PoE devices may not comply with the standards. QTECH switches provide the PoE command for compatibility with certain non-standard PoE devices.

Related Configuration

→ Enabling the Power Supply Function for a Port

By default, ports are enabled with the PoE power supply function.

You can run the **no poe enable** command to disable the PoE function for ports.

→ Configuring Power Supply Priorities for Ports

By default, the power supply priorities of ports are low.

You can run the **poe priority { low | high | critical }** command to configure the power supply priority of a port. If the power is insufficient, ports with high priorities preempt the power of ports with low priorities. In this case, certain ports with low priorities may be powered off due to insufficient power.

→ Configuring the Power Allocated to a Port

By default, the power allocated to a port is 0.

You can run the **poe alloc-power int** command to configure the power allocated to a port.

→ Configuring the Maximum Power for Ports

By default, there is no power restriction on ports.

You can run the **poe max-power int** command to configure the maximum power for a port.

→ Configuring the Regular Power-off Function for a Port

By default, ports do not have the regular power-off function.

You can run the **poe power-off time-range range-name** command to configure the regular power-off function for a port. In the clock period specified by **time-range**, the PoE switch does not supply power for connected PDs.

→ Configuring Compatibility with Non-standard PDs

By default, a PoE port is not compatible with non-standard PDs.

You can run the **poe legacy** command to enable compatibility with non-standard PDs.

13.3.4. Auxiliary PoE Power Supply Functions

Working Principle

The PoE MIB (RFC3621) standard provides **pethMainPseUsageThreshold** to set the power alarm threshold of the system.

PoE switches provide the CLI to set this value. The function of this CLI is the same as **pethMainPseUsageThreshold** MIB, which is setting the power alarm limit of the system. If the **pethNotificationControlEnable** switch is enabled in the MIB, the MIB receives notifications on the alarm power.

In actual application, whether the system sends trap notifications in case of power change and port power-on/off needs to be controlled. The **pethNotificationControlEnable** item is provided in the PoE standard MIB RFC3621, which is used to set whether to send trap notifications.

In actual application, you often have to record the PD connected to a specific PoE port. RFC3621 provides **pethPsePortType** to set the PD description.

PoE switches provide the CLI to set this value.

Related Configuration

→ Configuring the Power Alarm Threshold of the System

By default, the power alarm threshold of the system is 99.

You can run the **poewarning-power int** command to configure the power alarm threshold of the system.

→ Configuring the Trap Notification Sending Switch of the System

By default, the system disables sending of trap notifications.

You can run the **poenotification-control enable** command to enable trap notification sending of the system.

→ Configuring the PD Descriptor of a Port

By default, a port has no PD descriptor.

You can run the **poepd-description pd-name** command to configure the PD descriptor for the port.

13.3.5. LLDP Classification

Working Principle

According to the IEEE 802.3at standard, PDs supporting 802.3at must support both secondary hardware classification (which is 2-Event Physical Layer classification in the standard) and LLDP classification (which is Data Link Layer classification in the standard). A PD can identify itself as a Class4 type by exchanging LLDP packets with the PSE. The PSE needs to support only one classification. QTECH switches support LLDP classification.

After a PD of Class4 and Type2 is inserted into a PoE switch, the PoE switch performs detection and classification first and then supplies power for the PD. The PoE switch identifies a device as Type1 device and provides a maximum of 13 W power by default. After LLDP classification is performed, a PD can be identified as a Type2 device. If the PoE switch has sufficient power, the PD can obtain a maximum of 25.5 W power. If the PoE switch cannot allocate more power any longer, the PD will constantly send LLDP power request packets to request for power allocation.

The following table lists the maximum power that can be requested by PDs of each class.

Class	Type	Maximum Power (W)	Allocated Power (W)
Class 0	Type 1	13	15.4
Class 1	Type 1	3.9	4
Class 2	Type 1	6.5	7
Class 3	Type 1	13	15.4
Class 4	Type 1	13	15.4
Class 4	Type 2	25.5	30

Since the cable loss needs to be deducted from the power provided by the PSE, the allocated power is slightly higher than the maximum power requested by the PD.

This function is enabled by default and takes effect only in the auto mode.

Related Configuration

→ Configuring LLDP Classification

By default, the system disables the LLDP classification.

You can run the **poe class-ldp enable** command to enable LLDP classification.

13.4. Configuration

Configuration	Description and Command	
<u>Configuring PoE Power Supply on Line Cards</u>	🔥 (Mandatory) It is used to manage the PoE power supply on line cards.	
	poe enable [device device_num] slot slot_num	Enables the power supply function for line cards.
	poe priority { critical high low } [device device_num] slot slot_num	Configures power supply priorities for line cards.
	poe max-power max-power [device device_num] slot slot_num	Configures the maximum power that can be allocated to a line card.
<u>Configuring Power Supply of the PoE System</u>	🔥 (Mandatory) It is used to manage the PoE power supply of the system.	
	poe mode	Configures the power supply management mode.
	poe reserve-power	Configures the reserved power of the system.
	poe uninterruptible-power	Configures uninterruptible power supply during hot startup.

<u>Configuring Power Supply on PoE Ports</u>	<p>👉 (Mandatory) It is used to manage the PoE power supply of a specific port.</p>	
	poe enable	Enables the power supply function for a port.
	poe priority	Configures the power supply priority for the port.
	poe max-power	Configures the maximum power allocated to the port.
	poe alloc-power	Configures the power allocated to the port.
	poe power-off time-range name	Configures the regular power-off function for the port.
	poe legacy	Configures compatibility with non-standard PDs.
<u>Configuring Auxiliary PoE Power Supply Functions</u>	<p>👉 (Optional) It facilitates PoE system management.</p>	
	poe warning-power	Configures the power alarm threshold of the system.
	poe notification-control enable	Configures the trap notification sending switch of the system.
	poe pd-description	Configures the PD descriptor of a port.
<u>Enabling the LLDP Classification</u>	<p>👉 (Optional) It is used to manage the LLDP classification between the PoE and PDs.</p>	
	poe class-lldp enable	Uses the LLDP classification.

13.4.1. Configuring PoE Power Supply on Line Cards

Configuration Effect

- Configure a line card to enable or disable the PoE function. If the PoE function is disabled, all ports on the line card do not supply power externally.
- Configure priorities of line cards. If the power is insufficient, line cards with high priorities can preempt the power of line cards with low priorities but line cards with the same priority do not preempt the power from each other.
- Configure **max-power** that can be allocated to each line card.

Configuration Steps

➔ Enabling the Power Supply Function for Line Cards

- (Mandatory) It is enabled by default.
 - To enable or disable the PoE function for a line card, you must enable or disable the power supply function of the line card.
 - Line card-based configuration is supported.
- **Configuring Power Supply Priorities for Line Cards**
- (Mandatory) The priority is low by default.
 - In scenarios with insufficient power, in order to supply stable power for certain line cards, you can configure priorities for the line cards.
 - Line card-based configuration is supported.
- **Configuring Allocated Power for Line Cards**
- (Mandatory) It is enabled by default.
 - By configuring allocated power for line cards, you can meet varied requirements of PDs for the total power on the line cards.
 - Configure the maximum power for a line card. The default value varies with the number of line card ports. For a line card with 24 ports, the default power is 369.6 W; for a line card with 48 ports, the default power is 739.2 W.
 - If the remaining power of the PoE is smaller than the rated power of a new line card but is greater than 20% of the rated power of the line card, the remaining power will be allocated to the new line card; otherwise, 0 W will be allocated to the new line card.
 - Line card-based configuration is supported.

Verification

View the power supply status of the PoE system to check whether the configuration is correct and whether the configuration takes effect for the power supply.

Related Commands

→ Enabling the Power Supply Function for Line Cards

Command	poe enable pse [device <i>device_num</i>] slot <i>slot_num</i>
Parameter Description	<i>device_num</i> : In the standalone system, device is unavailable. In the VSU system, device indicates the corresponding chassis or cassette device. If device is not set, it indicates the master chassis or master device. <i>slot_num</i> : Indicates the slot number of the line card.
Command Mode	Global configuration mode
Usage Guide	-

→ Configuring Power Supply Priorities for Line Cards

Command	poe priority pse { low high critical } [device device_num] slot slot_num
Parameter Description	{ low high critical }: Indicates the priority. The value can be Low, High or Critical. device_num: In the standalone system, device is unavailable. In the VSU system, device indicates the corresponding chassis or cassette device. If device is not set, it indicates the master chassis or master device. slot_num: Indicates the slot number of the line card.
Command Mode	Global configuration mode
Usage Guide	-

→ Configuring Allocated Power for Line Cards

Command	poe max-power max-power pse [device device_num] slot slot_num
Parameter Description	max-power: Indicates the maximum power for a line card, ranging from 0 to 1440 W. device_num: In the standalone system, device is unavailable. In the VSU system, device indicates the corresponding chassis or cassette device. If device is not set, it indicates the master chassis or master device. slot_num: Indicates the slot number of the line card.
Command Mode	Global configuration mode
Usage Guide	-

Configuration Example

→ Configuring the Power Supply Management Policies for Line Cards

Scenario	<ul style="list-style-type: none"> The supply power is 1000 W. There are four line cards with the PoE function. Where, slot 1 needs a power of 300 W, slot 2 needs a power of 400 W, slot 3 needs a power of 0 W, and slot 4 needs a power of 400 W. The services deployed in slot 2 have the highest priority.
Configuration Steps	<ul style="list-style-type: none"> Set the power allocated to line card 1 to 300 W, the power allocated to line card 2 to 400 W, and the power allocated to line card 4 to 400 W. Disable the power supply function of line card 3. Set the power supply priority of line card 2 to high.
	<pre> QTECH# configure terminal QTECH(config)# poe max-power 300 pse slot 1 QTECH(config)# poe max-power 400 pse slot 2 QTECH(config)# poe max-power 400 pse slot 4 QTECH(config)# no poe enable pse slot 3 </pre>

	QTECH(config)# poe priority high pse slot 2
Verification	Run the show poe powersupply command to view the configurations and the power supply information.
	<pre> QTECH#show poe powersupply Device member : 1 Power management : auto PSE total power : 1000W PSE total power consumption : 1000W PSE total remain power : 0W PSE total powered port : 0 PSE disconnect mode : dc PSE reserve power : 0% PSE warning power : 99% PSE class lldp : disable PSE member : 1 PSE Power status : normal PSE Power Enabled : enable PSE max power : 300W PSE priority : low PSE alloc power : 300W PSE available power : 300W PSE total power consumption : 0 W PSE total remain power : 300W PSE peak power : 0 W PSE average power : 0 W PSE powered port : 0 PSE member : 2 PSE Power status : normal PSE Power Enabled : enable PSE max power : 400W PSE priority : high PSE alloc power : 400W PSE available power : 400W PSE total power consumption : 0 W PSE total remain power : 400W PSE peak power : 0 W </pre>

```
PSE average power          : 0 W
    PSE powered port       : 0
PSE member                 : 3
PSE Power status          : normal
PSE Power Enabled         : disable
PSE max power             : 369.6W
PSE priority              : low
PSE alloc power           : 0W
PSE available power       : 0W
PSE total power consumption : 0 W
PSE total remain power    : 0W
PSE peak power            : 0 W
PSE average power          : 0 W
    PSE powered port       : 0
PSE member                 : 4
PSE Power status          : normal
PSE Power Enabled         : enable
PSE max power             : 400W
PSE priority              : low
PSE alloc power           : 300W
PSE available power       : 300W
PSE total power consumption : 0 W
PSE total remain power    : 300W
PSE peak power            : 0 W
PSE average power          : 0 W
    PSE powered port       : 0
```

13.4.2. Configuring Power Supply of the PoE System

Configuration Effect

- Configure **mode** and change the power allocation mode for PDs. In the auto mode, power is allocated based on PD classes. In the energy-saving mode, power is allocated based on actual consumption.
- Configure **reserve-power**. In the energy-saving mode, the reserved power will not be allocated.
- Configure **uninterruptible-power**, which maintains the PoE power supply function during hot startup.

Configuration Steps

→ Configuring the Power Supply Management Mode

- (Mandatory) It is auto by default.
- Switch the power supply management mode, power off all PoE ports and then power on them based on the new power supply management mode.
- To ensure that the PoE switch powers more ports, you can use the energy-saving mode and allocate power to the ports based on actual power consumption.
- Support the global configuration and port-based configuration.

→ Configuring the Reserved Power of the System

- (Mandatory) It takes effect only in the energy-saving mode.
- Set the system reserved power command, which takes effect only when the current PoE switch is in the energy-saving mode.
- Setting the reserved power in the energy-saving mode may cause power-off of ports that have been powered on.
- Support the global configuration.

→ Configuring Uninterruptible Power Supply During Hot Startup

- (Optional) It is disabled by default.
- In actual application, switches may need to be upgraded. For example, after the management software is upgraded, a PoE switch needs to be restarted. However, many PDs are normally powered by the PoE switch in this case. Direct restart may cause power-off and then power-on of the PDs, that is, the PDs may be interrupted for a period of time.
- After this function is enabled or disabled, the configuration will take effect upon next reset only after being saved. If you forget to save the configuration or change the PoE configuration after saving, the system will remind you to save the configuration.
- Support the global configuration.

Verification

View the power supply status of the PoE system to check whether the configuration is correct and whether the configuration takes effect for the power supply.

Related Commands

→ Configuring the Power Supply Management Mode

Command	<code>po e mode { auto energy-saving }</code>
Parameter Description	{ <code>auto</code> <code>energy-saving</code> }: Indicates the auto and energy-saving modes.
Command Mode	Global configuration mode

Usage Guide	-
--------------------	---

→ Configuring the Reserved Power of the System

Command	poe reserve-power <i>int</i>
Parameter Description	<i>Int</i> : Indicates the percentage of the reserved power. <0~50>
Command Mode	Global configuration mode
Usage Guide	-

→ Configuring Uninterruptible Power Supply During Hot Startup

Command	poe uninterruptible-power
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	-

Configuration Example

→ Configuring the Power Supply Management Policies for the System

Scenario	<ul style="list-style-type: none"> Each of the connected PDs consumes low power, but the number of the connected PDs is large and all ports are occupied. The PDs should not be disconnected during hot startup.
Configuration Steps	<ul style="list-style-type: none"> Switch the mode to the energy-saving mode. Configure the reserved power of the system as 20%. Support uninterruptible power supply during hot startup.
	<pre>QTECH# configure terminal QTECH(config)# poe mode energy-saving QTECH(config)# poe reserve-power 20 QTECH(config)# poe uninterruptible-power QTECH(config)# exit QTECH# write</pre>
Verification	Run the show poe powersupply command to view the configurations and the power supply information.

```
QTECH#show poe powersupply
Device member                : 1
Power management             : energy-saving
PSE total power              : 1000W
PSE total power consumption  : 369.6W
PSE total remain power      : 630.4W
PSE total powered port      : 0
PSE disconnect mode         : dc
PSE reserve power           : 20%
PSE warning power           : 99%
PSE class lldp              : disable
    PSE member               : 1
    PSE Power status         : normal
    PSE Power Enabled        : enable
    PSE max power            : 369.6W
    PSE priority             : low
    PSE alloc power          : 369.6W
    PSE available power      : 295.7W
    PSE total power consumption : 0 W
    PSE total remain power   : 295.7W
    PSE peak power          : 0 W
    PSE average power        : 0 W
    PSE powered port        : 0
```

13.4.3. Configuring Power Supply on PoE Ports

Configuration Effect

- Configure **time-range** to ensure that ports are not powered off within the time-range.
- Configure **priority** for ports. If the power is insufficient, ports with high priorities can preempt the power of ports with low priorities but ports with the same priority do not preempt the power from each other.
- Configure **legacy** to be compatible with non-standard PD devices.
- Configure **max-power** for ports. If the power consumed by a port exceeds 1.1 times of the max-power, the power is powered off. After a penalty period of 10 seconds, the port is powered on again.
- Configure **alloc-power** for ports. In the static mode, power is allocated to ports based on alloc-power.

Configuration Steps

→ Enabling the Power Supply Function for a Port

- (Mandatory) It is enabled by default.
- To enable or disable the PoE function for a port, you must enable or disable the power supply function of the port.
- By default, the PoE function of the port for connecting a convergence switch is enabled and the PoE function for a core switch is disabled.
- If you run the interface range command to configure the PoE function for ports in batches, the enabling or disabling of the PoE function for a port may affect the global power supply management because the range command is configured for ports one after another. Therefore, ports may be powered on and then off during the configuration process, which is normal.
- Support port-based configuration.

→ Configuring the Regular Power-off Function for a Port

- Optional.
- When the power supply function is enabled for a port, configure time-range and then manage the power-on/off of the port based on the period of time specified by range-name.
- The accuracy of the regular power supply function for a PoE port is one minute and 30 seconds.
- Configure the regular power-off function for a PoE port. range-name indicates the name of the time range, consisting of up to 32 characters.
- Support port-based configuration.

→ Configuring the Power Supply Priority for a Port

- (Mandatory) The priority of a port is low by default.
- In scenarios with insufficient power, in order to supply stable power for certain ports, you can configure priorities for the ports.
- Support the global configuration and port-based configuration.

→ Configuring Compatibility with Non-standard PDs

- (Optional) It is not supported by default.
- If connected PDs do not meet the PoE standard, the function of being compatible with non-standard PDs can be enabled to supply power for the PDs.
- Running this command for ports not connected to PDs may cause burning of peer devices due to incorrect power-on. Therefore, you must run this command when PDs are connected to ports.
- Class 0 is displayed for all non-standard PoE devices.

- If this command is not configured, non-standard PDs connected will not be powered on and the system will not display any prompt information.
- Support port-based configuration.

→ Configuring the Maximum Power Allocated to a Port

- (Optional) There is no maximum power restriction on a port by default.
- This command may take effect in the auto and energy-saving modes.
- When max-power is set to 0, a port is powered off and not powered on again.
- For a PoE switch supporting only 802.3af, the value of max-power ranges from 0 to 15.4.
- Configure the maximum power of a port. The maximum power cannot exceed 1.1 times of the configured power to reduce the impact of high power consumed by a single port on power management.
- Support port-based configuration.

→ Configuring the Power Allocated to a Port

- If the system power is insufficient when power allocated to a port is configured, the system prompts that the configuration fails.
- Support port-based configuration.

Verification

View the PoE information of PoE ports to check whether the configuration is correct and whether the configuration takes effect for the power supply.

Related Commands

→ Enabling the Power Supply Function for a Port

Command	poe enable
Parameter Description	-
Command Mode	Interface configuration mode
Usage Guide	-

→ Configuring the Regular Power-off Function for a Port

Command	poe power-off time-range <i>name</i>
Parameter Description	<i>name</i> : Indicates the descriptor of time-range.
Command Mode	Interface configuration mode

Usage Guide	-
--------------------	---

→ Configuring Power Supply Priorities for Ports

Command	poe priority { low high critical }
Parameter Description	{ low high critical }: Indicates the priority. The value can be Low, High or Critical.
Command Mode	Interface configuration mode
Usage Guide	-

→ Configuring Compatibility with Non-standard PDs

Command	poe legacy
Parameter Description	-
Command Mode	Interface configuration mode
Usage Guide	-

→ Configuring the Maximum Power Allocated to a Port

Command	poe max-power int
Parameter Description	<i>Int</i> : Indicates the maximum power, ranging from 0 to 30 W. The value ranges from 0 to 15.4 for a system supporting only 802.3af.
Command Mode	Interface configuration mode
Usage Guide	-

→ Configuring the Power Allocated to a Port

Command	poe alloc-power int
Parameter Description	<i>Int</i> : Indicates the maximum power, ranging from 0 to 30 W.
Command Mode	Interface configuration mode
Usage Guide	-

Configuration Example

➔ Configuring the Power Supply Management Policies for a Port

<p>Scenario</p>	<ul style="list-style-type: none"> • The port g0/1 requires a stable power supply not affected by the network environment. • The power is powered off from 8:00 to 12:00 and is powered on in other time. • The maximum power of the port does not exceed 17 W.
<p>Configuration Steps</p>	<ul style="list-style-type: none"> • Set the priority of the port g0/1 to critical. • Configure time-range and associate the port time-range configuration of the PoE. • Set the maximum power of the port g0/1 to 15.4 W.
	<pre>QTECH# configure terminal QTECH(config)# time-range poe-time QTECH(config-time-range)# periodic daily8:00 to 12:00 QTECH(config-time-range)# exit QTECH(config)# interface gigabitEthernet 0/1 QTECH(config-if)# poe power-off time-range poe-time QTECH(config-if)# poe priority critical QTECH(config-if)# poe max-power 15.4</pre>
<p>Verification</p>	<p>Run the show poe interface gigabitEthernet 0/1 command to view the configurations and the power supply information.</p>
	<pre>QTECH#show poe interface gigabitEthernet 0/1 Interface : gi0/1 Power enabled : enable Power status : on Max power : 15.4W Allocate power : N/A Current power : 14.8 W Average power : 14.8 W Peak power : 14.8 W LLDP requested power : 0 W LLDP allocated power : 0 W Voltage : 53.5 V Current : 278 mA PD class : 4 Trouble cause : None</pre>

```
Priority           : critical
Legacy            : off
Power-off time-range : poe-time
Power management  : auto
```

13.4.4. Configuring Auxiliary PoE Power Supply Functions

Configuration Effect

- Configure **warning-power** to display a warning when the power used by the system exceeds the alarm threshold.
- Configure **notification-control** to control whether the system sends trap notifications in case of power change and port power-on/off.
- Configure **pd-description** to identify the PD connected to a port.

Configuration Steps

→ Configuring the Power Alarm Threshold of the System

- (Mandatory) It is 99 by default, which is consistent with that specified in the RFC3621 MIB.
- Configure the power alarm threshold of the system. When the power used by the system exceeds the threshold, the system displays a warning.
- If you set the power alarm threshold of the system by using `pethMainPseUsageThreshold` provided by the PoE MIB, the CLI will be configured as well.
- Support the global configuration.

→ Configuring the Trap Notification Sending Switch of the System

- (Mandatory) It is disabled by default.
- When trap notification sending is enabled, trap notifications will be sent when the alarm power notification and power on/off notification of the system are enabled and disabled.
- This CLI command can control only sending of trap notifications defined in the RFC3621 and does not take effect for trap notifications not defined in the RFC3621.
- When sending of trap notifications defined in the RFC3621 is enabled, a notification is sent if the alarm power changes from being lower than or equal to the system power to being higher than the system power. If the alarm power is always higher than the system power, no trap notification will be sent. If the alarm power changes from being higher than or equal to the system power to being lower than the system power, no trap notification will be sent if the alarm power is always lower than the system power subsequently.
- Support the global configuration and port-based configuration.

→ Configuring the PD Descriptor of a Port

- (Optional) A port has no PD descriptor by default.
- Configure the PD descriptor of a port to easily identify the PD connected to the port.
- If you set the PD by using **pethPsePortType** provided by the MIB, the CLI will be configured as well.
- Support port-based configuration.

Verification

Check whether alarm information is output when the power used by the system fluctuates on the alarm power threshold to check whether the alarm power configuration takes effect.

Connect the PoE to the SNMP server and power on and off a port to check whether corresponding trap notifications are received from the server and check whether the trap configuration takes effect.

View the PoE information of the port to check whether the PD descriptor of the port is correct.

Related Commands

→ Configuring the Power Alarm Threshold of the System

Command	poewarnig-power int
Parameter Description	<i>Int</i> : Indicates the alarm power percentage, ranging from 0 to 99.
Command Mode	Global configuration mode
Usage Guide	-

→ Configuring the Trap Notification Sending Switch of the System

Command	poenotification-control enable
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	-

→ Configuring the PD Descriptor of a Port

Command	poepd-description pd-name
Parameter Description	<i>pd-name</i> : Indicates the PD descriptor name. The parameter value is a string and supports a maximum of 32 characters.

Command Mode	Interface configuration mode
Usage Guide	-

Configuration Example

→ Configuring the Power Supply Management Policies for the System

Scenario	<ul style="list-style-type: none"> When the system power exceeds 80%, a warning should be displayed. When a port is powered on or off, trap notifications should be sent. PDs connected to ports can be identified.
Configuration Steps	<ul style="list-style-type: none"> Set the alarm power threshold of the system to 80%. Enable the trap notification sending switch of the system. Configure the PD descriptor of the port g0/1 as ap220.
	<pre>QTECH# configure terminal QTECH(config)# poe poe warnig-power 80 QTECH(config)# poe notification-control enable QTECH(config)# interface gigabitEthernet 0/1 QTECH(config-if)# poe pd-description ap220</pre>
Verification	Run the show running-config command to view the configurations and power supply information.

13.4.5. Enabling the LLDP Classification

Configuration Effect

- Configure **class-lldp** to support power supply and power negotiation through LLDP between a PoE switch and PDs.

Notes

Configuration Steps

→ Using the LLDP Classification

- (Optional) It is disabled by default.
- The system switches to the auto mode. Enable the LLDP classification function in the global configuration mode and verify that there is no max-power configuration on the ports.
- If a power is configured with the **Max-power** command to restrict the maximum power, the LLDP power adjustment function of the port fails.
- A PoE switch does not allow PDs to adjust their priorities through LLDP requests. The port priorities are managed by the PoE switch in a unified manner.

- Support port-based configuration.

Verification

View the "PD class" information in the PoE information of a port to check whether the port is in the LLDP correlation with PDs.

Related Commands

→ Using the LLDP Classification

Command	poe class-lldp enable
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	-

Configuration Example

→ Configuring the Power Supply Management Policies for a Port

Scenario	Correlate a PD of Class4 with the PSE.
Configuration Steps	Enable the LLDP classification.
	<pre>QTECH# configure terminal QTECH(config)# poe class-lldp enable</pre>
Verification	Run the show poe interface gigabitEthernet 0/1 command to view the configurations and the power supply information.
	<pre>QTECH#show poe interface gigabitEthernet 0/1 Interface : gi0/1 Power enabled : enable Power status : on Max power : 15.4W Allocate power : N/A Current power : 14.8 W Average power : 14.8 W Peak power : 14.8 W LLDP requested power : 0 W LLDP allocated power : 0 W Voltage : 53.5 V</pre>

```
Current           : 278 mA
PD class          : 4 (Type1)
Trouble cause     : None
Priority           : critical
Legacy            : off
Power-off time-range : poe-time
Power management  : auto
```

13.5. Monitoring

Displaying

Description	Command
Displays the PoE configuration and status of a specified port.	show poe interface
Displays the PoE status or configurations of all ports.	show poe interfaces
Displays the power supply status of the current PoE system.	show poe powersupply

14. CONFIGURING UFT

14.1. Overview

The unified forwarding table (UFT) enables the switch to dynamically allocate the hardware forwarding entries.

Protocols and Standards

N/A

14.2. Applications

Typical Application	Scenario
<u>Dynamic Entry Allocation</u>	When a device operates in common routing mode, the MPLS label is not required for forwarding and the corresponding entry capacity is not used. If the entry capacity of the MPLS label can be used by other entries, such as ARP/ND entries, the device can learn more ARP/ND entries.

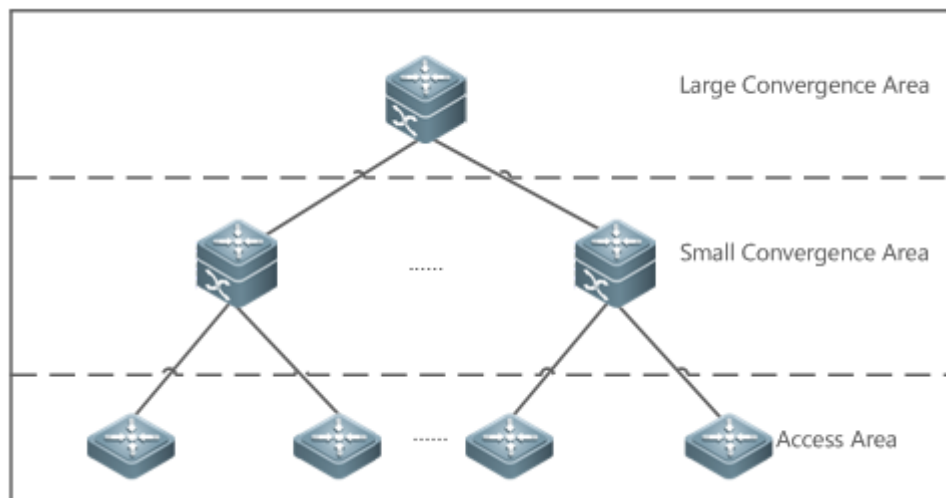
14.2.1. Dynamic Entry Allocation

Scenario

The following figure shows the simple and common topology of the campus network. The core device may be deployed in the small convergence area as a small convergence device. Layer 2 functions of the core device are mainly enabled. The core device can also be deployed in the large convergence area as a large convergence device. In this case, the core device works as a gateway. When the core device acts as a small convergence device, it requires a large enough size of the MAC address table.

Another application scenario of the core device is acting as a large convergence device, namely, a large gateway. Its access capability depends on the ARP and ND capacity, namely, the number of IPv4 and IPv6 terminals that can be accessed. Take the device installed with Windows7 operating system as an example. Such a device supports IPv4 and IPv6 dual-stack. When a terminal accesses the device, the terminal occupies one ARP entry and one ND entry. In this application scenario, a great number of ARP and ND entries are required.

Figure 14-1



Deployment

- Enable the switch to operate in Bridge mode of UFT to increase the MAC address table capacity.
- Enable the switch to operate in Gateway mode of UFT to increase the ARP and ND entry capacity.

14.3. Features

Basic Concepts

N/A

Overview

Feature	Function
<u>UFT operating mode</u>	The UFT provides a mechanism for users to select an operating mode to meet the application scenario needs.

14.3.1. UFT Operating Mode

Working Principle

The UFT provides a mechanism for users to select an operating mode to meet the application scenario needs.

The UFT supports up to eight operating modes. The selected operating mode can take effect after it is saved and the device is restarted.

→ Default

By default, the UFT mode of the switch is Default. In Default mode, each hardware entry of the switch is applied to most of application scenarios.

→ Bridge

The Bridge mode is the Layer 2 forwarding mode. It is applied to the application scenarios in which pure Layer 2 services dominate. In Bridge mode, ARP, ND and MPLS capacity is greatly reduced and most of capacity is allocated to the MAC address table.

→ Gateway

The Gateway mode is classified into three modes: gateway mode, gateway-max mode, and gateway-ndmax mode.

Gateway mode is applied to the application scenarios in which Layer 3 services dominate. Gateway-max mode is applied to the application scenarios in which a large number of terminals are deployed. Gateway-ndmax mode is applied to the application scenarios in which a large number of IPv6 terminals are deployed.

→ Route

The Route mode is the network routing mode. It is applied to the application scenarios in which a great amount of routing and forwarding dominate.

The Route mode is classified into route-v4max and route-v6max modes. In these two modes, the IPv6 and IPv6 network routing table capacity are respectively allocated to maximum extent.

→ Label

The Label mode is MPLS mode. In Label mode, the MAC address, ARP and ND table capacity are reduced, while MPLS table capacity increases.

14.4. Configuration

Configurati on Item	Suggestions and Related Commands	
Configuring UFT Operating Mode	Optional configuration. Switch over the current UFT operating mode of the switch.	
	<code>switch-mode mode_type slot slot_num</code>	Switches the UFT operating mode in stand-alone mode.
	<code>switch-mode mode_type switch switch_num slot slot_num</code>	Switches the UFT operating mode in VSU mode.

14.4.1. Configuring UFT Operating Mode

Configuration Effect

- Configure the Bridge mode to increase the Layer 2 entry size. The Bridge mode is applied to the application scenarios in which Layer 2 services dominate.
- Configure the Gateway mode to increase the ARP and ND table size. The Gateway mode is applied to the application scenarios in which Layer3 services dominate.
- Configure the Route mode to increase the routing table size. The Route mode is applied to the application scenarios that require a great amount of routing and forwarding.

Notes

- After configuration is complete, save it and restart the device to validate configuration.
- The UFT function may result in automatic restart of the line card once.

Configuration Method

→ Switching the UFT Operating Mode in Stand-Alone Mode

Mandatory configuration.

Use the **switch-mode** *mode_type* **slot** *slot_num* command to switch the UFT mode of the switch.

Command Syntax	switch-mode <i>mode_type</i> slot <i>slot_num</i>
Parameter Description	<i>mode_type</i> : UFT operating mode. <i>slot_num</i> : indicates the corresponding line card installed in the chassis.
Defaults	Default mode
Command Mode	Global configuration mode
Usage Guide	<p>👉 In stand-alone mode, the line card can operate in the following modes:</p> <ul style="list-style-type: none"> ● default: Default mode, which is applied to most of application scenarios. ● bridge: Bridge mode, which is applied to the application scenarios where pure Layer 2 services dominate. ● gateway: Gateway mode, which is applied to the application scenario in which Layer 3 services dominate. ● gateway-max: Gateway-max mode, which is applied to the application scenarios in which a large number of terminals are deployed. ● gateway-ndmax: Gateway-ndmax mode, which is applied to the application scenarios in which a large number of IPv6 terminals are deployed. ● label: Label mode, which is applied to the application scenarios that require a great amount of MPLS. ● route-v4max: IPv4 routing mode, which is applied to the application scenarios that require a great number of IPv4 routes.

- **route-v6max**: IPv6 routing mode, which is applied to the application scenarios that require a great number of IPv6 routes.

→ Switching the UFT Operating Mode in VSU Mode

Mandatory configuration.

Use the **switch-mode mode_type switch switch_num slot slot_num** command to switch the UFT mode of the switch.

Command Syntax	switch-mode mode_type switch switch_num slot slot_num
Parameter Description	<i>mode_type</i> : UFT operating mode. <i>switch_num</i> : In stand-alone mode, the switch keyword is invisible. In VSU mode, the switch keyword indicates the chassis or box device. <i>slot_num</i> : indicates the line card installed in the chassis device.
Defaults	Default mode
Command Mode	Global configuration mode
Usage Guide	<p>👉 In VSU mode, the line card can operate in the following modes:</p> <ul style="list-style-type: none"> ● default: Default mode, which is applied to most of application scenarios. ● bridge: Bridge mode, which is applied to the application scenarios where pure Layer 2 services dominate. ● gateway: Gateway mode, which is applied to the application scenarios in which Layer 3 services dominate. ● gateway-max: Gateway-max mode, which is applied to the application scenarios in which a large number of terminals are deployed. ● gateway-ndmax: Gateway_ndmax mode, which is applied to the application scenarios in which a large number of IPv6 terminals are deployed. ● label: Label mode, which is applied to the application scenarios that require a great amount of MPLS. ● route-v4max: IPv4 routing mode, which is applied to the application scenarios that require a great number of IPv4 routes. ● route-v6max: IPv6 routing mode, which is applied to the application scenarios that require a great number of IPv6 routes.

Verification

- After the device is restarted, use the show run command to display the current line card status and check whether the configuration takes effect.
- Use the **show switch-mode status** command to display the UFT mode status.

Command Syntax	show switch-mode status
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, interface configuration mode
Usage Guide	N/A
Configuration Example	<pre>QTECH(config)#show switch-mode status Slot No Switch-Mode switch 1 slot 3 bridge</pre>

Configuration Examples

→ Switching UFT Operating Mode in Stand-Alone Mode

Network Environment	N/A
Configuration Method	Switch the UFT operating mode of the line card in slot3 of the switch to Bridge mode.
	<pre>QTECH(config)#switch-mode bridge slot 3 Please save current config and restart your device! QTECH(config)#show run Building configuration... Current configuration : 1366 bytes version 11.0(1B2) ! cwmmp ! install 3 QSW-M7600-48GT4XS-EB ! sysmac 08c6.b334.5624 ! nfpp ! switch-mode bridge slot 3</pre>
Check Method	Use the show switch-mode status command to display configuration information.

```
QTECH(config)#show switch-mode status
Slot No           Switch-Mode
3                 bridge
```

Common Errors

-

14.5. Monitoring

Clearing

N/A

Displaying the Running Status

Function	Command
Displays UFT operating mode of the switch	show switch-mode status

Displaying Debugging Information

-

- ↪ The preceding monitoring and maintaining commands are also valid to the chassis devices and box devices, in stand-alone mode and VSU mode.
- ↪ In stand-alone mode, the **switch** keyword is invisible. For the chassis device, **slot** keyword indicates a specified line card.

15. CONFIGURING PKG_MGMT

15.1. Overview

Package management (pkg_mgmt) is a package management and upgrade module. This module is responsible for installing, upgrading/degrading, querying and maintaining various components of the device, among which upgrade is the main function. Through upgrade, users can install new version of software that is more stable or powerful. Adopting a modular structure, the RGOS system not only supports overall upgrade and subsystem upgrade but also supports separate upgrade of a feature package. In addition, the RGOS system supports upgrade through hot patches.

↪ Component upgrade described in this document applies to both the box-type device and rack-type device. In addition, this document is for only version 11.0 and later, excluding those upgraded from earlier versions.

Protocols and Standards

N/A

15.2. Applications

Application	Scenario
Upgrading/Degrading Subsystem	Upgrade subsystem firmware like boot, kernel, and roots on the box-type device and rack-type device.
Upgrading/Degrading a Single Feature Package	Upgrade a single feature package on the box-type device and rack-mount device.
Installing a Hot Patch Package	Install a hot patch, and repair a certain part of the feature component.
Auto-Sync for Upgrade	Configure the auto sync policy, range and path.

15.2.1. Upgrading/Degrading Subsystem

Scenario

After the upgrade of a subsystem firmware is complete, all system software on the device is updated, and the overall software is enhanced. The subsystem firmware of the rack-mount device is called rack package.

The main features of this upgrade mode are as follows: All software on the device is updated after the upgrade is completed; all known software bugs are fixed. It takes a long time to finish upgrade.

Deployment

You must store the rack package in a USB flash drive before performing the upgrade because the rack package is too large to be stored in the memory space of the device.

15.2.2. Upgrading Subsystem by One-click

Scenario

Upgrade the firmware automatically without interrupting services on a VSU system. While either in VSU mode or in standalone mode, one single device will restart after this configuration, thus interrupting services.

Deployment

You must store the rack package in a USB flash drive before performing the upgrade because the rack package is too large to be stored in the memory space of the device.

15.2.3. Upgrading/Degrading a Single Feature Package

Scenario

Device software consists of several components, and each component is an independent feature module. After an independent feature package is upgraded, only the feature bug corresponding to this package is fixed. Besides, this feature is enhanced with the other features unchanged.

The features of this upgrade mode are as follows: Generally, a feature package is small and the upgrade speed is high. After the upgrade is completed, only the corresponding functional module is improved, and other functional modules remain unchanged.

Deployment

You can store this package in the root directory of the TFTP server, download the package to the local device, and then complete the upgrade. You can also store the package in a USB flash drive, connect the USB flash drive to the device, and then complete the upgrade.

15.2.4. Installing a Hot Patch Package

Scenario

To fix software bugs without restarting the device, you can install hot patch packages. Hot patch packages are only applicable to fixing a specific software version. Generally, hot patch packages are released to fix the software of a certain version only when the device cannot be started in the user's environment.

The most significant feature of hot patch upgrade is that all bugs can be fixed without device restart after the upgrade is completed.

Deployment

You can store this package in the root directory of the TFTP server, download the package to the local device, and then complete the upgrade. You can also store the package in a USB flash drive, connect the USB flash drive to the device, and then complete the upgrade.

15.2.5. Auto-Sync for Upgrade

Scenario

Auto-sync upgrade aims to ensure the coordination of multiple modules (line cards and chassis) within a system on a rack-type device or VSU. Specifically, the upgrade firmware is pushed to all target members automatically and the software version of new members is upgraded automatically based on the auto-sync policy.

Deployment

- Configure the policy for auto-sync upgrade.
- Configure the path of firmware for auto-sync upgrade.

15.3. Features

Basic Concepts

→ Subsystem

A subsystem exists on a device in the form of images. The subsystems of the RGOS include:

- boot: After being powered on, the device loads and runs the boot subsystem first. This subsystem is responsible for initializing the device, and loading and running system images.
- kernel: kernel is the OS core part of the system. This subsystem shields hardware composition of the system and provides applications with abstract running environment.
- rootfs: rootfs is the collection of applications in the system.

→ Rack Package

A rack package is used to upgrade a subsystem component of the rack-type device. This type of package contains the main packages of the supervisor module and all line cards. Therefore, a rack package can be used to upgrade all line cards on a rack-type device once for all.

→ Feature Package of RGOS

The feature package of RGOS refers to a collection which enables a certain feature. When the device is delivered, all supported functions are contained in the rootfs subsystem. You can upgrade only a specific feature by upgrading a single feature package.

→ Hot Patch Package

A hot patch package contains the hot patches of several features. You can upgrade a hot patch package to install patches for various features. New features are provided immediately without device restart after the upgrade.

👉 "Firmware" in this document refers to an installation file that contains a subsystem or feature module.

Overview

Feature	Description
Upgrading/Degrading and Managing Subsystem Components	Upgrades/degrades a subsystem.
Upgrading/Degrading and Managing Functional Components	Upgrades/degrades a functional component.
Upgrading/Degrading and Managing Hot Patch Packages	Installs a hot patch package.
Auto-Sync for Upgrade	Ensures uniform upgrade upon member change.

15.3.1. Upgrading/Degrading and Managing Subsystem Components

Subsystem upgrade/degradation aims to upgrade the software by replacing the subsystem components of the device with the subsystem components in the firmware. The subsystem component contains redundancy design. Subsystems of the device are not directly replaced with the subsystems in the package during upgrade/degradation in most cases. Instead, subsystems are added to the device and then activated during upgrade/degradation.

Working Principle

→ Upgrade/Degradation

Various subsystems exist on the device in different forms. Therefore, upgrade/degradation varies with different subsystems.

- boot: Generally, this subsystem exists on the norflash device in the form of images. Therefore, upgrading/degrading this subsystem is to write the image into the norflash device.
- kernel: This subsystem exists in a specific partition in the form of files. Therefore, upgrading/degrading this subsystem is to write the file.

- rootfs: Generally, this subsystem exists on the nandflash device in the form of images. Therefore, upgrading/degrading this subsystem is to write the image into the nandflash device.

→ Management

Query the subsystem components that are available currently and then load subsystem components as required.

Each subsystem component contains redundancy design. During the upgrade/degradation:

- boot: The boot subsystem always contains a master boot subsystem and a slave boot subsystem. Only the master boot subsystem is involved in the upgrade, and the slave boot subsystem serves as the redundancy backup all along.
- kernel: as the kernel subsystem contains at least one redundancy backup. More redundancy backups are allowed if there is enough space.
- rootfs: The rootfs subsystem always contains a redundancy backup.

The boot component is not included in the scope of subsystem management due to its particularity. During upgrade of the kernel or rootfs subsystem component, the upgrade/degradation module always records the subsystem component in use, the redundant subsystem component, and management information about various versions.

Relevant Configuration

→ Upgrade

Store the upgrade file on the local device, and then run the upgrade command for upgrade.

15.3.2. Upgrading/Degrading and Managing Functional Components

Working Principle

In fact, upgrading a feature is replacing feature files on the device with the feature files in the package.

Managing feature components and hot patches is aimed at recording the information of feature components and hot patches by using a database. In fact, installing, displaying and uninstalling a component is the result of performing the Add, Query and Delete operation on the database.

After package upgrade, component upgrade cannot be performed.

Relevant Configuration

→ Upgrade

- Store the upgrade file on the local device, and then run the upgrade command for upgrade.

15.3.3. Upgrading/Degrading and Managing Hot Patch Packages

Working Principle

In fact, upgrading a feature component is replacing feature files on the device with the feature files in the package.

Upgrading hot patch packages is similar to upgrading features. The difference is that only files to be revised are replaced during hot patch package upgrade. In addition, after the files are replaced, the new files take effect automatically.

After package upgrade, component upgrade cannot be performed.

Management

Similar to feature component management, hot patch management also includes the query, installation, and uninstallation operation, which is the result of adding, querying and deleting data respectively.

Hot patches and feature components are managed based on the same technology. The difference is that the hot patches involve three different states, that is, Not installed, Installed, and Activated. These states are described as follows:

The hot patch in Installed state only indicates that this hot patch exists on the device, but it has not taken effect yet.

Only the hot patch in Activated state is valid.

Relevant Configuration

→ Upgrade

- Store the upgrade file in the local file system, and then run the upgrade command for upgrade.

→ Activating a Hot Patch

- You can run the **patch active** command to activate a patch temporarily. The patch becomes invalid after device restart. To use this patch after device restart, you need to activate it again.
- You can also run the **patch running** command to activate a patch already permanently. The patch is still valid after device start.
- The patch not activated will never become valid.

→ Deactivating a Hot Patch

- To deactivate an activated patch, run the **patch deactivate** command.

→ Uninstalling a Hot Patch

- You can run the **patch delete** command to uninstall a hot patch.

15.3.4. Auto-Sync for Upgrade

Working Principle

Auto-sync upgrade aims to ensure the coordination of multiple modules (line cards and chassis) within a system. Specifically, the upgrade firmware is pushed to all target members automatically and the software version of new members is upgraded automatically based on the auto-sync policy.

There are three policies available.

None: No auto-sync upgrade.

Compatible: Performs auto-synchronization based on the sequential order of versions.

Coordinate: Synchronizes with the version based on the firmware stored on the supervisor module.

Auto-sync is performed in the following scenarios:

If no upgrade target is specified, the firmware is pushed to all matching members (including line cards and chassis) for auto-sync.

Every member is checked when the device is restarted and auto-sync is performed accordingly.

Every new member is checked when added into the system and auto-sync is performed accordingly.

→ Management

Auto-upgrade policy, range and path should be configured in advance.

Relevant Configuration

→ Configuring Auto-Sync Policy

To perform upgrade as expected, check the configuration in advance, such as the path.

If some line cards are not checked for upgrade because the system is not configured with auto-sync policy. You can upgrade them manually.

15.4. Configuration

Configuration	Description and Command
Upgrading/Degrading a Firmware	<p>👉 The basic function of the configuration is installing and upgrading/degrading a subsystem firmware, feature package, and hot patch package. This command is valid on both the box-type device and rack-type device.</p>
	<p><code>upgrade [slot { num M1 M2 all }] url [force]</code> <i>url</i> is a local path where the firmware is stored. This command is used to install and upgrade the firmware stored on the device.</p>

	upgrade download tftp://path	<i>path</i> is the path of the firmware on the server. This command is used to download a firmware from the server and upgrade the package automatically.
	upgrade rollback	Rolls back subsystem firmware.
	patch active	Activates a patch temporarily.
	patch running	Activates a patch permanently,
<u>Deactivating and Uninstalling a Hot Patch</u>	(Optional) Deactivates or uninstalls a hot patch.	
	patch deactivate	Deactivates an activated patch.
	patch delete	Uninstalls a hot patch.
<u>Auto-Sync for Upgrade</u>	(Optional) Configures auto-sync policy.	
	upgrade auto-sync policy	Configures the auto-sync policy.
	upgrade auto-sync range	Configures the auto-sync range.
	upgrade auto-sync package	Configures the auto-sync path.

15.4.1. Upgrading/Degrading a Firmware

Configuration Effect

Available firmwares include the rack package, various feature packages and hot patch packages.

- After the upgrade of the rack package is complete, all system software on the rack-type device is updated, and the overall software is enhanced.
- After an independent feature package is upgraded, only the feature bug corresponding to this package is fixed. Besides, this feature is enhanced, with other features remain unchanged.
- Upgrading hot patch packages is aimed at fixing software bugs without restarting the device. Hot patch packages are only applicable to fixing bugs for a specific version of software.

↳ Generally a rack package is released to upgrade a rack-type device.

Notes

N/A

Configuration Steps

→ Upgrading a Rack Package

- Optional configuration. This configuration is required when all system software on the device needs to be upgraded.

- When using a rack package to upgrade subsystem components, you must store the rack package in a USB flash drive and then run the upgrade command because the rack package is very large.

↳ Generally a rack package is pushed to upgrade a rack-type device.

→ Upgrading Rack Packages for VSU by One-Click

- Optional configuration. This configuration is required when all system software of the VSU device needs to be upgraded.
- Download the package to the local device and run the upgrade auto command.

↳ Generally a rack package is pushed to upgrade a rack-type device.

→ Upgrading Each Feature Package

- Optional configuration. The configuration is used to fix bugs of a certain feature and enhance the function of this feature.
- Download the package to the local device and run the upgrade command.

→ Upgrading a Hot Patch Package

- Optional configuration. The configuration is used to fix software bugs without restarting the device.
- Download the package to the local device and run the upgrade command.
- After being upgraded, the hot patch can be used after it is activated. The configuration in this step is mandatory. Two activation modes are available: Run the patch active command to activate a patch temporarily, or run the **patch running** command to activate a patch permanently.

↳ Generally, the **patch running** command must be used to activate a patch permanently in the user scenario. The **patch active** command can be used to activate a patch only when a user intends to verify the patch.

→ Subsystem Rollback

- Optional configuration. This configuration aims to roll a subsystem back to the state before the upgrade, select this configuration item.
- This configuration takes effect after you run the **upgrade** command to upgrade the subsystem component (for example, the rack package).

↳ After you run the upgrade command to upgrade a subsystem component in the user scenario, you can run the rollback command once, that is, consecutive rollback is not supported.

Verification

- After upgrading a subsystem component, you can run the **show upgrade history** command to check whether the upgrade is successful.
- After upgrading a feature component, you can run the **show component** command to check whether the upgrade is successful.
- After upgrading a hot patch package, you can run the **show patch** command to check whether the upgrade is successful.

Commands

→ Upgrading Package

Command	upgrade [slot { num M1 M2 all }] url [force]
Parameter Description	slot indicates that this command is executed on the device in the specified slot; num indicates the slot number of the specified line card; M1 and M2 indicate the supervisor modules; all indicates all devices. <i>url</i> indicates the path of the firmware in the device file system. force indicates forced upgrade.
Command Mode	Privileged EXEC mode
Usage Guide	Before upgrade, run the copy command to copy the package to the file system If you use this command without specifying parameters, all matched components will be upgraded.

Command	upgrade download tftp:/path
Parameter Description	<i>path</i> indicates the path of the firmware in the device file system.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

→ Displaying the Firmware Stored on the Device

Command	show upgrade file url
Parameter Description	<i>url</i> indicates the path of the firmware in the device file system.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

→ Viewing the Device Upgrade Process

Command	show upgrade status
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	This command is available on only the rack-type device, and it is used to display the upgrade status of each line card.

→ **Displaying Upgrade History**

Command	show upgrade history
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

→ **Subsystem Component Rollback**

Command	upgrade rollback [slot { num M1 M2 all }]
Parameter Description	slot indicates that this command is executed on the device in the specified slot; <i>num</i> indicates the slot number of the specified line card; M1 and M2 indicate the supervisor modules; all indicates all devices.
Command Mode	Privileged EXEC mode
Usage Guide	This command is used to undo the last subsystem upgrade operation and make the subsystem restore to the state before the upgrade. You can perform the rollback operation only if the last upgrade is subsystem upgrade and the upgrade is successful. The rollback command cannot be executed in succession. 🔗 All parameters are applicable to only the rack-type device.

→ **Upgrading a Firmware Automatically without Interrupting Services**

Command	upgrade auto url [force]
Parameter Description	<i>url</i> : Firmware directory force : Enforces upgrade.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to upgrade the VSU system. Download the program of the latest version to the device before running this command (by using the copy tftp command).

	<p>During one upgrade, do not use the upgrade auto command and other upgrade commands (such as the upgrade command) at the same time. If auto-upgrade fails, follow the system prompt to restore the version.</p> <p>Do not update the firmware (by running the copy tftp command/U disk copy) or perform other upgrade operation (running the upgrade /upgrade auto command) repetitively.</p> <p>During auto-upgrade, do not unplug the card, perform hot backup switchover, power off chassis or change VSU software/hardware configuration.</p>
--	---

→ Displaying the Feature Components Already Installed

Command	show component [slot { num M1 M2 all }] [component_name]
Parameter Description	<p>[component_name]: component name</p> <p>When this parameter value is N/A, the command is used to display all components already installed on the device and basic information of these components.</p> <p>When this parameter value is not N/A, the command is used to display detailed information of the corresponding component, check whether the component is intact, and check whether this component works properly.</p> <p>slot indicates that this command is executed on the device in the specified slot; num indicates the slot number of the specified line card; M1 and M2 indicate the supervisor modules; all indicates all devices.</p>
Command Mode	Privileged EXEC mode
Usage Guide	<p>↪ All parameters are applicable to only the rack-type device.</p>

→ Displaying the Patch Packages Already Installed

Command	show patch [slot { num M1 M2 all }] [package_name]
Parameter Description	<p>slot indicates that this command is executed on the device in the specified slot; num indicates the slot number of the specified line card; M1 and M2 indicate the supervisor modules; all indicates all devices.</p>
Command Mode	Privileged EXEC mode
Usage Guide	<p>↪ All parameters are applicable to only the rack-type device.</p>

→ Activating the Patches Temporarily

Command	patch active [slot { num M1 M2 all }]
Parameter Description	<p>slot indicates that this command is executed on the device in the specified slot; num indicates the slot number of the specified line card; M1 and M2 indicate the supervisor modules; all indicates all devices.</p>
Command Mode	Privileged EXEC mode

Usage Guide	<p>This operation can be performed only on the device already installed with a patch. This command can be used to activate a patch temporarily, and the activated patch becomes invalid after device restart.</p> <hr/> <p>↪ All parameters are applicable to only the rack-type device.</p>
--------------------	--

→ **Activating the Patches Permanently**

Command	patch running [slot { num M1 M2 all }]
Parameter Description	slot indicates that this command is executed on the device in the specified slot; <i>num</i> indicates the slot number of the specified line card; M1 and M2 indicate the supervisor modules; all indicates all devices.
Command Mode	Privileged EXEC mode
Usage Guide	<p>This operation can be performed only on the device already installed with a patch. This command can be used to activate a patch permanently.</p> <hr/> <p>↪ All parameters are applicable to only the rack-type device.</p>

Configuration Example

→ **Example of Upgrading a Main Package for a VSU**

Network Environment	<p>Before the upgrade, you must copy the firmware to the device. The upgrade module provides the following solutions.</p> <ul style="list-style-type: none"> ● Run some file system commands like copy tftp and copy xmodem to copy the firmware on the server to the device file system, and then run the upgrade auto url command to upgrade the firmware in the local file system. ● Copy the firmware to a USB flash drive, Insert the USB flash drive to the device, and then run the upgrade auto url command to upgrade the firmware in the USB flash drive.
Configuration Steps	<ul style="list-style-type: none"> ● Run the upgrade auto command. ● The VSU active and standby devices are restarted in sequence.
	<pre> 2015-04-09_09-56-23 QTECH#upgrade auto usb0:S7600_RGOS12.3(5)B1_install.bin 2015-04-09_09-56-24 QTECH#*Jan 1 00:23:40: %7: 2015-04-09_09-56-24 *Jan 1 00:23:40: %7: [Slot 1/0]:Upgrade processing is 10% 2015-04-09_09-56-26 QTECH#show upgrade status 2015-04-09_09-56-26 [Slot 1/0] 2015-04-09_09-56-26 dev_type: s6k 2015-04-09_09-56-26 status : upgrading </pre>

```
2015-04-09_09-56-26 [Slot 2/0]
2015-04-09_09-56-26      dev_type: s6k
2015-04-09_09-56-26      status  : transmission
2015-04-09_09-58-20 *Jan   1  00:25:36: %7: [Slot 2/0]:Upgrade
processing is 10%
2015-04-09_09-58-30 QTECH#show upgrade status
2015-04-09_09-58-30 [Slot 1/0]
2015-04-09_09-58-30      dev_type: s6k
2015-04-09_09-58-30      status  : upgrading
2015-04-09_09-58-30 [Slot 2/0]
2015-04-09_09-58-30      dev_type: s6k
2015-04-09_09-58-30      status  : upgrading
2015-04-09_09-58-39 *Jan   1  00:25:56: %7:
2015-04-09_09-58-39 *Jan   1  00:25:56: %7: [Slot 2/0]:Upgrade
processing is 60%
2015-04-09_09-59-19 *Jan   1  00:26:35: %7:
2015-04-09_09-59-19 *Jan   1  00:26:35: %7: [Slot 2/0]:Upgrade
processing is 90%
2015-04-09_09-59-19 *Jan   1  00:26:35: %7:
2015-04-09_09-59-19 *Jan   1  00:26:35: %7: [Slot 2/0]:
2015-04-09_09-59-19 *Jan   1  00:26:35: %7: Upgrade info [OK]
2015-04-09_09-59-19 *Jan   1  00:26:36: %7:           Kernel
version[2.6.32.6b311610a8eb91->2.6.32.6b31161115502c]
2015-04-09_09-59-19 *Jan   1  00:26:36: %7:           Rootfs
version[1.0.0.eb75cd01->1.0.0.3d978b6c]
2015-04-09_09-59-19 *Jan   1  00:26:36: %7:
2015-04-09_09-59-19 *Jan   1  00:26:36: %7: [Slot 2/0]:Reload system to
take effect!
2015-04-09_09-59-21 *Jan   1  00:26:37: %7:
2015-04-09_09-59-21 *Jan   1  00:26:37: %7: [Slot 2/0]:Upgrade
processing is 100%
2015-04-09_10-00-28 QTECH#show upgrade status
2015-04-09_10-00-28 [Slot 1/0]
2015-04-09_10-00-28      dev_type: s6k
2015-04-09_10-00-28      status  : upgrading
2015-04-09_10-00-28 [Slot 2/0]
2015-04-09_10-00-28      dev_type: s6k
2015-04-09_10-00-28      status  : success
2015-04-09_10-01-39 *Jan   1  00:28:56: %7:
```

	<pre> 2015-04-09_10-01-39 *Jan 1 00:28:56: %7: [Slot 1/0]:Upgrade processing is 60% 2015-04-09_10-02-17 *Jan 1 00:29:33: %7: 2015-04-09_10-02-17 *Jan 1 00:29:33: %7: [Slot 1/0]:Upgrade processing is 90% 2015-04-09_10-02-17 *Jan 1 00:29:33: %7: 2015-04-09_10-02-17 *Jan 1 00:29:33: %7: [Slot 1/0]: 2015-04-09_10-02-17 *Jan 1 00:29:34: %7: Upgrade info [OK] 2015-04-09_10-02-17 *Jan 1 00:29:34: %7: Kernel version[2.6.32.6b311610a8eb91->2.6.32.6b31161115502c] 2015-04-09_10-02-17 *Jan 1 00:29:34: %7: Rootfs version[1.0.0.eb75cd01->1.0.0.3d978b6c] 2015-04-09_10-02-17 *Jan 1 00:29:34: %7: 2015-04-09_10-02-18 *Jan 1 00:29:34: %7: [Slot 1/0]:Reload system to take effect! 2015-04-09_10-02-19 *Jan 1 00:29:35: %7: 2015-04-09_10-02-19 *Jan 1 00:29:35: %7: [Slot 1/0]:Upgrade processing is 100% 2015-04-09_10-02-19 *Jan 1 00:29:36: %7: %PKG_MGMT:auto-sync config synchronization, Please wait for a moment.... 2015-04-09_10-02-20 *Jan 1 00:29:36: %7: 2015-04-09_10-02-20 [1784.116069] rtc-pcf8563 6-0051: retrieved date/time is not valid. 2015-04-09_10-02-20 *Jan 1 00:29:36: %7: [Slot 2/0]:auto sync config: space not enough left 57229312, need 114597815 2015-04-09_10-02-20 *Jan 1 00:29:36: %7: 2015-04-09_10-02-20 *Jan 1 00:29:36: %7: [Slot 2/0]:auto sync package config err 2015-04-09_10-02-20 *Jan 1 00:29:37: %7: [Slot 1/0] 2015-04-09_10-02-21 *Jan 1 00:29:37: %7: device_name: s6k 2015-04-09_10-02-21 *Jan 1 00:29:37: %7: status: SUCCESS 2015-04-09_10-02-21 *Jan 1 00:29:37: %7: [Slot 2/0] 2015-04-09_10-02-21 *Jan 1 00:29:37: %7: device_name: s6k 2015-04-09_10-02-21 *Jan 1 00:29:37: %7: status: SUCCESS 2015-04-09_10-02-21 *Jan 1 00:29:38: %7: %Do with dtm callback.... 2015-04-09_10-02-21 *Jan 1 00:29:38: %VSU-5-DTM_AUTO_UPGRADE: Upgrading the system, wait a moment please. </pre>
Verification	If the version information changes, the upgrade is successful.
	QTECH#show version

```

System description      : Qtech High-density IPv6 100G Core Routing
Switch(QSW-7608)
System start time      : 2021-03-02 08:32:22
System uptime          : 0:10:37:42
System hardware version : 1.00
System software version : QSW-7600_OS 12.3(1)B0202
System patch number    : NA
System serial number    : G1P90ZQ001654
System boot version     : 1.3.25(Master) 1.3.25(Slave)
System rboot version    : 1.1.18
Module information:
  Slot M1 : QSW-M7608-CM
    System uptime      : 0:10:37:42
    Hardware version    : 1.00
    Boot version        : 1.3.25(Master) 1.3.25(Slave)
    Rboot version       : 1.1.18
    Software version    : QSW-7600_OS 12.3(1)B0202
    Serial number       : G1P90ZQ001654
  Slot 2 : QSW-M7600-48GT4XS-EB
    System uptime      : 0:10:37:54
    Hardware version    : 1.02
    Boot version        : 1.3.21(Master) 1.3.21(Slave)
    Rboot version       : 1.0.5
    Software version    : QSW-7600_OS 12.3(1)B0202
    Serial number       : G1PDBZL10100A
    
```

→ Example of Upgrading a Subsystem Firmware on the Rack-Type Device

<p>Network Environment</p>	<p>Generally, a rack-type device is supplied with a USB flash drive. Before installing a rack package, you need to store the rack package into the USB flash drive. The upgrade module provides the following solutions.</p> <ul style="list-style-type: none"> ● Run some file system commands like copy tftp and copy xmodem to copy the firmware on the server to the device file system, and then run the upgrade url command to upgrade the firmware in the local file system. ● Copy the firmware to a USB flash drive, connect the USB flash drive to the device, and then run the upgrade url command to upgrade the firmware in the USB flash drive.
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ● Run the upgrade command. ● You can view the line card status during the upgrade.

- After upgrading the subsystem, restart the device for the upgrade to take effect.

```
QTECH# upgrade usb0:/ca-octeon_11.0(1B2)_20131106_main_install.bin
[Slot M1]:Upgrade processing is 10%

[Slot 1]:Upgrade processing is 10%

[Slot M1]:Upgrade processing is 60%

[Slot 1]:Upgrade processing is 60%

[Slot M1]:Upgrade processing is 90%

[Slot M1]:
Upgrade info [OK]
  Kernel version[2.6.32.abb2b41f170c81->2.6.32.abb2b415749f40]
  Rootfs version[1.0.0.d5f0de03->1.0.0.660e0085]

[Slot M1]:Reload system to take effect!

[Slot M1]:Upgrade processing is 100%
[Slot 1]:Upgrade processing is 90%

[Slot 1]:
Upgrade info [OK]
  Kernel version[2.6.32.9f8b56f1d45ab2 ->2.6.32.0f48cb9f170c81]
  Rootfs version[1.0.0.2ad02537->1.0.0.1bcc12e8]

[Slot 1]:Restart to take effect !

[Slot 1]:Upgrade processing is 100%
[slot: M1]
  device_name: ca-octeon-cm
  Status:      SUCCESS
[slot: 1]
  device_name: ca-octeon-lc
  status:     SUCCESS
```


	<pre>QTECH#show upgrade status [slot: M1] dev_type: ca-octeon-cm status : upgrading [slot: 1] dev_type: ca-octeon-lc status : transmission</pre>
Verification	<pre>Reload system?(Y/N)y Restarting system.</pre>
	<ul style="list-style-type: none"> ● Check the system version on the current device. If the version information changes, the upgrade is successful.
	<pre>QTECH#show upgrade history Last Upgrade Information: Time: 2014-08-31 12:15:03 Method: LOCAL Package Name: QSW-7600_RGOS11.0(1)B1_CM_01200616_install.bin Package Type: Distribution</pre>

→ Example of Upgrading a Feature Package on the Rack-Type Device

Network Environment	<p>Generally, a rack-type device is supplied with a USB flash drive. Before installing a rack package, you need to store the rack package into the USB flash drive. The upgrade module provides the following solutions.</p> <ul style="list-style-type: none"> ● Run some file system commands like copy tftp and copy xmodem to copy the firmware on the server to the device file system, and then run the upgrade url command to upgrade the firmware in the local file system. ● Copy the firmware to a USB flash drive, connect the USB flash drive to the device, and then run the upgrade url command to upgrade the firmware in the USB flash drive.
Configuration Steps	<ul style="list-style-type: none"> ● Run the upgrade command. ● Check whether the device needs to be restarted based on the prompt displayed after the upgrade.
	<pre>QTECH#upgrade sata0://ca-octeon-cm_bridge-1.0.0.05151504-1311060616.mips.rpm [Slot M1]:Upgrade processing is 10%</pre>

	<pre>[Slot M1]:Upgrade processing is 60% [Slot M1]: Upgrade info [OK] bridge version[1.0.0.97521231->1.0.0.05151504] [Slot M1]:Restart to take effect ! [Slot M1]:Upgrade processing is 100% [slot: M1] device_name: ca-octeon-cm status: SUCCESS [slot: M2] device_name: ca-octeon-lc status: NOT SUPPORT Reload system?(Y/N)y [1586.114348] Restarting system.</pre>
<p>Verification</p>	<ul style="list-style-type: none"> ● Check the version of the feature component on the current device. If the version information changes, the upgrade is successful.
	<pre>QTECH# show component slot M1 [Slot M1]: Package : bridge Version: 1.0.0.05151504 Build time: Wed May 15 07:05:06 2013 Size: 11 Install time: Thu Jan 1 00:48:09 1970 Description: bridge component Required packages: None -----</pre>

➔ Example of Installing a Patch Package on the Rack-Type Device

<p>Network Environment</p>	<p>Generally, a rack-type device is supplied with a USB flash drive. Before installing a rack package, you need to store the rack package into the USB flash drive. The upgrade module provides the following solutions.</p> <ul style="list-style-type: none"> ● Run some file system commands like copy tftp and copy xmodem to copy the firmware on the server to the device file system, and then run the upgrade url command to upgrade the firmware in the local file system.
----------------------------	---

	<ul style="list-style-type: none">● Copy the firmware to a USB flash drive, connect the USB flash drive to the device, and then run the upgrade url command to upgrade the firmware in the USB flash drive.
Configuration Steps	<ul style="list-style-type: none">● Run the upgrade command.● Activate the hot patch.
	<pre>QTECH#upgrade usb0:/ca-octeon-cm_RGOS11.0(1C2)_20131008_patch.bin [Slot M1]: Upgrade processing is 10% [Slot M1]: Upgrade processing is 60% [Slot M1]: Upgrade info [OK] patch_bridge version[1.0.0.1952] Upgrade processing is 90% [Slot M1]: Upgrade info [OK] patch_install version[1.0.0.192e35a] [slot: M1] device_name: ca-octeon-cm status: SUCCESS [slot: M2] device_name: ca-octeon-lc status: NOT SUPPORT QTECH#patch running slot M1 The patch on the system now is in running status</pre>
Verification	<ul style="list-style-type: none">● Check the hot patches installed on the current device.
	<pre>QTECH# show patch slot M1 [Slot M1]: Patch package patch_install installed in the system, version:pa1 Package : patch_bridge Status : running Version: pa1 Build time: Mon May 13 09:03:07 2013 size: 277 Install time: Tue May 21 03:07:17 2013 Description: a patch for bridge Required packages: None</pre>

→ Example of Subsystem Rollback on the Rack-Type Device

- 👉 You can perform the rollback operation only if the last upgrade is subsystem upgrade and the upgrade is successful. The rollback command cannot be executed in succession.
- 👉 The rack-type device allows you to perform the rollback operation on a specified line card.

Network Environment	<p>Generally, a rack-type device is supplied with a USB flash drive. Before installing a rack package, you need to store the rack package into the USB flash drive. The upgrade module provides the following solutions.</p> <ul style="list-style-type: none">● Run some file system commands like copy tftp and copy xmodem to copy the firmware on the server to the device file system, and then run the upgrade url command to upgrade the firmware in the local file system.● Copy the firmware to a USB flash drive, connect the USB flash drive to the device, and then run the upgrade url command to upgrade the firmware in the USB flash drive.
Configuration Steps	<ul style="list-style-type: none">● Run the subsystem rollback command.● Restart the device for the rollback to take effect.
	<pre>QTECH#upgrade rollback slot M1 kernel rollback version[2.6.32.abb2b415749f40- >2.6.32.abb2b41f170c81] [OK] rootfs rollback version[1.0.0.660e0085->1.0.0.d5f0de03] [OK] Rollback success! Reload system to take effect! Reload system?(Y/N) y Restarting system.</pre>
Verification	<ul style="list-style-type: none">● Check the system version on the current device. If it is restored to the version before the upgrade, the rollback is successful.
	<pre>QTECH#show upgrade history Last Upgrade Information: Time: 2014-08-31 12:15:03 Method: LOCAL Package Name: QSW-7600_RGOS11.0(1)B1_CM_01200616_install.bin Package Type: Distribution</pre>

Common Errors

If an error occurs during the upgrade, the upgrade module displays an error message. The following provides an example:

```
Upgrade info [ERR]
```

```
Reason:creat config file err(217)
```

The following describes several types of common error messages:

- Invalid firmware: The cause is that the firmware may be damaged or incorrect. It is recommended to obtain the firmware again and perform the upgrade operation.
- Firmware not supported by the device: The cause is that you may use the firmware of other devices by mistake. It is recommended to obtain the firmware again, verify the package, and perform the upgrade operation.
- Insufficient device space: Generally, this error occurs on a rack-type device. It is recommended to check whether the device is supplied with a USB flash drive. Generally, this device has a USB flash drive.

15.4.2. Deactivating and Uninstalling a Hot Patch

Configuration Effect

An activated hot patch is deactivated or uninstalled.

Notes

A hot patch that is not activated does not take effect; therefore, you cannot deactivate it.

Configuration Steps

→ Deactivating an Activated Patch

- Optional configuration. To deactivate an activated patch, run the patch deactivate command.

→ Uninstalling a Hot Patch

- Optional configuration. To uninstall a hot patch already installed, run the patch delete command.


Verification

- You can run the **show patch** command to check whether a patch is activated or uninstalled.


Commands

→ Deactivating an Activated Patch

Command	<code>patch deactivate [slot { num M1 M2 all }]</code>
Parameter Description	slot: indicates that this command is executed on the device in the specified slot. num: indicates the slot number of the specified line card. M1 and M2: indicate the supervisor modules. all: indicates all devices.
Command Mode	Privileged EXEC mode

Usage Guide	<p>You can perform this operation on only an activated patch.</p> <p> All parameters are applicable to only the rack-type device.</p>
--------------------	--

→ Deleting a Hot Patch

Command	patch delete [slot { num M1 M2 all }]
Parameter Description	<p>slot num: This parameter is used on a rack-type device. It indicates a corresponding line card based on the slot number.</p> <p>slot all: This parameter is used on a rack-type device. It indicates all devices.</p> <p>slot M1: This parameter is used on a rack-type device. It specifies that the operation is performed on supervisor module M1.</p> <p>slot M2: This parameter is used on a rack-type device. It specifies that the operation is performed on supervisor module M2.</p>
Command Mode	Privileged EXEC mode
Usage Guide	<p>This command is used to remove the hot patch package from the device.</p> <p> All parameters are applicable to only the rack-type device.</p>

Configuration Example

→ Deactivating and Uninstalling a Patch on the Box Device

Configuration Steps	<ul style="list-style-type: none"> ● Run the patch deactivation command. ● Run the patch deletion command.
Verification	<ul style="list-style-type: none"> ● Display patch status.
Configuration Steps	<pre>QTECH#patch deactivate Deactivate the patch package success QTECH# patch delete Clear the patch patch_bridge success Clear the patch success</pre>
Verification	<pre>QTECH#show patch No patch package installed in the system</pre>

→ Deactivating and Uninstalling a Patch on the Rack-Type Device

Configuration Steps	<ul style="list-style-type: none"> ● Run the patch deactivation command. ● Run the patch deletion command.
Configuration Steps	<pre>QTECH#patch deactivate slot M1 [Slot M1]:</pre>

	<pre>Deactivate the patch package success QTECH# patch delete slot M1 [Slot M1]: Clear the patch patch_bridge success Clear the patch success</pre>
Verification	<ul style="list-style-type: none">● Display patch status.
	<pre>QTECH#show patch slot M1 [Slot M1]: No patch package installed in the system</pre>

Common Errors

- Run the **patch deactivate** command when the patch is not activated. It is recommended to check the patch status. You can run the **patch deactivate** command only when the patch is in the **status:running** state.

15.4.3. Auto-Sync for Upgrade

Configuration Effect

Auto-sync policy, range and path is configured.

Notes

N/A

Configuration Steps

→ Configuring Auto-Sync Policy

Run the **upgrade auto-sync policy command** to configure the auto-sync policy. There are three modes available:

None: No auto-sync upgrade.

Compatible: Performs auto-synchronization based on the sequential order of versions.

Coordinate: Synchronizes with the version based on the firmware stored on the supervisor module.

→ Configuring Auto-Sync Range

Run the **upgrade auto-sync range command** to configure the auto-sync range. There are two ranges available:

chassis: Performs auto-sync on a chassis.

vsd: Performs auto-sync in the VSU system.

→ Configuring Auto-Sync Path

Every time the system is upgraded, the firmware path is recorded automatically for later auto-sync upgrade. Alternatively, use the **upgrade auto-sync package** command to set a path.

Verification

Run the upgrade auto-sync command to check the configuration.

Commands

→ Configuring Auto-Sync Policy

command	upgrade auto-sync policy [none compatible coordinate]
Parameter Description	none: No auto-sync upgrade compatible: Performs auto-synchronization based on the sequential order of versions. coordinate: Synchronizes with the version based on the firmware stored on the supervisor module.
Command Mode	Privileged EXEC mode
Usage Guide	It is recommended to set coordinate . ☞ All parameters are applicable to only the box-type device and VSU.

→ Configuring Auto-Sync Range

command	upgrade auto-sync range [chassis vsu]
Parameter Description	chassis: Performs auto-sync on a chassis. VSU: Performs auto-sync in the VSU system.
Command Mode	Privileged EXEC mode
Usage Guide	It is recommended to set VSU to ensure uniformity. ☞ All parameters are applicable to only the box-type device and VSU.

→ Configuring Auto-Sync Path

command	upgrade auto-sync package url
Parameter Description	<i>url</i> indicates the path of the firmware in the device file system.
Command Mode	Privileged EXEC mode
Usage Guide	The path is not set generally. ☞ All parameters are applicable to only the rack-type device and VSU.

Configuration Example

→ Configuring Auto-Sync Policy

Configurati on Steps	Configure the auto-sync policy.
	<pre>QTECH# upgrade auto-sync policy coordinate Upgrade auto-sync policy is set as coordinate</pre>
Verification	Check the auto-sync policy.
	<pre>QTECH#show upgrade auto-sync auto-sync policy: coordinate auto-sync range: vsu auto-sync package: flash:/eg1000m_main_1.0.0.0f328e91.bin</pre>

→ Configuring Auto-Sync Range

Configurati on Steps	Configure the auto-sync range.
	<pre>QTECH# upgrade auto-sync range vsu Upgrade auto-sync range is set as vsu.</pre>
Verification	Check the auto-sync range.
	<pre>QTECH#show upgrade auto-sync auto-sync policy: coordinate auto-sync range: vsu auto-sync package: flash:/eg1000m_main_1.0.0.0f328e91.bin</pre>

Common Errors

url is not valid.

15.5. Monitoring

Clearing

Function	Command
Deletes a hot patch package already installed.	patch delete [slot { num M1 M2 all }]

Displaying

Function	Command
Displays all components already installed on the current device and their information.	show component [slot { num M1 M2 all }] [component _name]

Displays the information about the hot patch packages already installed on the device.	show patch [slot { num M1 M2 all }] [patch _name]
Displays the upgrade status of various line cards on a rack-type device.	show upgrade status
Displays the upgrade history.	show upgrade history

16. CONFIGURING OPENFLOW

16.1. Overview

OpenFlow is a network transmission protocol that separates the forwarding plane from the control plane of network devices so that the network devices can focus on forwarding. The control of an entire network is then concentrated on one controller, which generates and sends forwarding rules in a flow table to the network devices using the OpenFlow protocol, thereby centrally managing the control plane and reducing maintenance and management costs.

Protocol Specification

- OpenFlow Switch Specification Version 1.0.0

16.2. Typical Application

Typical Application	Scenario
<u>Centralized Control</u>	Perform centralized management of authentication.

16.2.1. Centralized Control

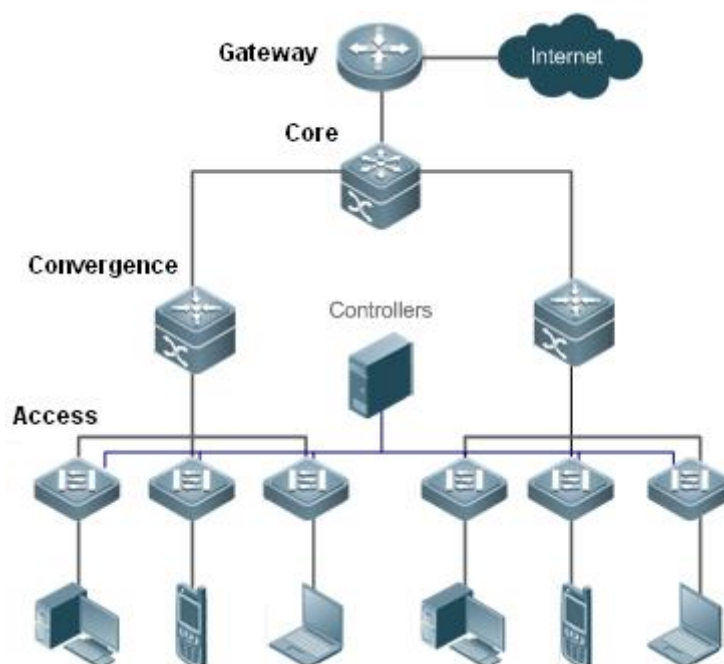
Application Scenario

The OpenFlow protocol can be used to perform centralized management of authentication on access devices.

As shown in the figure below, deploy a controller above access devices to control the authentication function of access devices, so that the authentication function (on the control plane) moves from the access devices to the controller.

- The controller asks an access device to send an authentication packet to itself using OpenFlow protocol.
- The controller completes the authentication process, and sends authentication results to the access device using the OpenFlow protocol to perform admission control on end users.

Figure 16-1



Function Deployment

- Run OpenFlow Client on the access devices to interconnect the access devices to the controller.
- Run OpenFlow Server on the controller to perform device discovery and management.

16.3. Function Details

→ Basic Concepts

Flow Table

The flow table is a core data structure for a network device to control forwarding policies. The network device determines, based on the flow table, a corresponding action to be taken for network traffic that enters the network device itself.

According to the OpenFlow protocol, the flow table consists of three parts: header, counter, and action.

- **Header:** It defines the index of the flow table and consists of various packet fields to match defined flows. These fields include but are not limited to the source MAC address, destination MAC address, Ethernet protocol type, source IP address, destination IP address, IP protocol type, source port, and destination port.
- **Counter:** It is used to count matched traffic.
- **Action:** It is the forwarding action to deal with the matched traffic, and includes but is not limited to discarding, broadcasting, and forwarding.

→ Message

The OpenFlow protocol supports three categories of messages: controller-to-switch, asynchronous, and symmetric. Each message category further includes several types of sub-messages. The three categories of messages are described as follows:

- **controller-to-switch**: initiated by the controller to manage and obtain the network device status.
- **asynchronous**: initiated by a network device to update network events or network device status changes (most commonly link up/down of a network port) to the controller.
- **Symmetric**: initiated either by a switch or the controller for initial handshake and connection status detection of the protocol.

Features

Feature	Function
<u>Separating Control from Forwarding</u>	Separate the data layer from the control layer of a network device.
<u>STP Control</u>	Set whether STP management is performed by a Software Defined Network (SDN) controller or the local device.

16.3.1. Separating Control from Forwarding

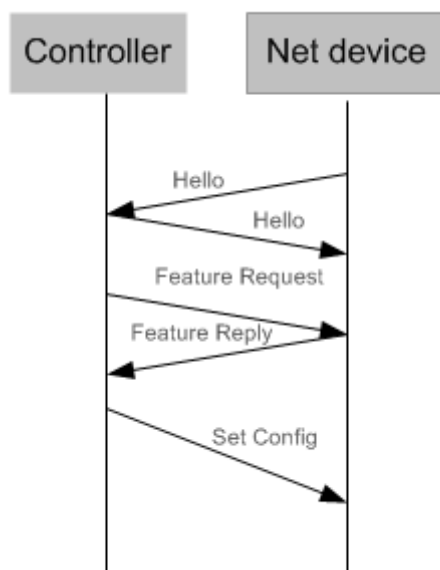
Perform centralized management of the network control plane, so that the entire network is centrally managed at ease (as compared with the status quo of the network), thereby reducing maintenance and management costs.

Working Principle

The OpenFlow protocol runs over Transport Layer Security (TLS) or unprotected TCP connections, and defines the interaction between the controller and network devices. The controller sends flow table information to the network devices, so as to control the method for forwarding network data packets and some configuration parameters. Each network device will send a notification message to the controller when its link is interrupted or when the network device receives a data packet in which no forwarding action has been specified. In this way, the interaction between the controller and the network devices is implemented to eventually control the transmission of the entire network.

The process of discovering each other shall be completed before the controller and a network device interact with each other. Figure 16-2 shows the specific actions involved in this process.

Figure 16-2



Hello packets are sent between the controller and the network device to achieve a handshake. When the handshake is done, the controller requests specific information about the network device, including (but not limited to) the number of ports on the network device and the capability of each port (such as the Feature Request/Reply shown in Figure 16-2). Then the controller delivers specific user configurations (such as Set Config shown in Figure 16-2) to the network device. After a connection is established, the controller defines various flows and corresponding actions for the flows, and delivers them in a flow table to the network device. When a data packet enters the network device, the network device matches the data packet with the flow table according to present flow table rules and performs a corresponding action (including forwarding, discarding, and modifying the packet). At the same time, a corresponding counter is updated. If no match is found in the flow table, the network device forwards the data packet to the controller.

The network device locally maintains the flow table delivered from the controller. If the data packet to be forwarded is already defined in the flow table, the network device directly forwards the data packet. Otherwise, the data packet is sent to the controller to confirm the transmission path (which can be understood as control plane parsing to generate the flow table) and then forwarded based on the flow table delivered from the controller.

Related Configuration

→ Default Configuration

The OpenFlow protocol is disabled by default.

→ Enabling/Disabling OpenFlow to Connect/Disconnect the Controller

- Run the **of controller-ip** command to enable OpenFlow.
- Run the **no of controller-ip** command to disable OpenFlow.

16.3.2. STP Control

According to the OpenFlow protocol, the Spanning Tree Protocol (STP) function of a network device allows the network device to be managed either locally or through an

SDN controller. Therefore, a configuration command is required to perform switching between the two management methods. The configuration command takes effect only when OpenFlow management is enabled.

If loop control is enabled on the controller, do not enable the STP function on a network device; otherwise, the two functions conflict with each other. Enable the STP function on the network device only when loop control is disabled on the controller and a loop probably exists in the network device. After the STP function is enabled on the network device, STP configuration is further required on the network device. For details, see the section about STP configuration.

Working Principle

A network device communicates with the controller using the OFPC-STP field that is carried in an OFPT_FEATURES_REPLY message of the OpenFlow protocol to decide which subject will currently perform STP management. When the controller performs STP management according to the configuration, all STP-related processing is performed by the controller; otherwise, the network device itself performs the processing in a conventional way.

Related Configuration

→ Default Configuration

The STP function is provided by the controller by default.

→ Enabling STP Management on the SDN Controller or Local Device

- Run the **of stp** command to set STP management performed by the SDN controller.
- Run the **no of stp** command to set STP management performed by the local network device.

16.4. Configuration Details

Action	Suggestions and Related Commands
<u>Configuring OpenFlow</u>	👉 Mandatory configuration, which is used to enable OpenFlow.
	of controller-ip Enables the OpenFlow function
	no of controller-ip Disables the OpenFlow function
<u>Configuring OpenFlow STP</u>	👉 Optional configuration, which is used to enable the STP function of the SDN controller as necessary.
	of stp Enables the STP management function on the SDN controller.
	no of stp Enables the STP management function on the local device.

16.4.1. Configuring OpenFlow

Configuration Effect

- Trigger the network device to establish a connection with the specified controller and eventually establish an OpenFlow management channel.

Notes

- Before switching the address of the controller, disable and then enable the OpenFlow function again.

Configuration Method

→ Enabling the OpenFlow Function

- This configuration is required for enabling OpenFlow.

→ Disabling the OpenFlow Function

- This configuration is required for switching the controller or disabling the OpenFlow function.

→ Displaying the Connection Status Between the OpenFlow Device and the Controller

- Display the connection status between the current device and the controller.

Verification

- Display the connection status of current protocol using the show of command.

Related Commands

→ Enabling the OpenFlow Function

Command Syntax	of controller-ip ip-address [port port-value] interface [interface-id]
Parameter Description	controller-ip ip-address: controller IP address. port port-value: port that connects to the controller. The default value is 6633. Interface interface-id: port ID, which can be either an out-of-band management interface or a common in-band physical Ethernet interface.
Command Mode	Global configuration mode
Usage Guide	-

→ Disabling the OpenFlow Function

Command Syntax	no of controller-ip
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	Run this command before switching the controller.


→ Enabling or Disabling the Local STP Function on the OpenFlow Device

Command Syntax	of stp
-----------------------	---------------

Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	Run this command to select enabling the local STP function on the network device or enabling the STP function on the OpenFlow controller.

Configuration Examples

➔ Configuring the IP Address and Access Port (6633 by Default) of the Controller to Connect the Network Device

Network Environment Figure 16-3																																																													
Configuration Method	<ul style="list-style-type: none"> ● Enable the OpenFlow function on the network device and specify the controller IP address. 																																																												
	<pre>QTECH# configure terminal QTECH(config)# interface mgmt 0 QTECH(config-if)# ip address 172.18.2.36 255.255.255.0 QTECH(config-if)# exit QTECH(config)# of controller-ip 172.18.2.35 interface mgmt 0</pre>																																																												
Verification	<ul style="list-style-type: none"> ● Display the connection status between the OpenFlow device and the controller, port status and flow table status. 																																																												
	<pre>QTECH# show of Controller is 172.18.2.35 port 6633,connected. QTECH#show of port STP is controlled by SDN Controller.</pre> <table border="1"> <thead> <tr> <th>PORTID</th> <th>IFX</th> <th>COFIG</th> <th>STATE</th> <th>LINK</th> <th>SPEED</th> </tr> </thead> <tbody> <tr> <td>DUPLEX</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>1</td> <td>1</td> <td>0x0000</td> <td>0x0001</td> <td>0</td> <td>0</td> </tr> <tr> <td>2</td> <td>2</td> <td>0x0000</td> <td>0x0001</td> <td>0</td> <td>0</td> </tr> <tr> <td>3</td> <td>3</td> <td>0x0000</td> <td>0x0001</td> <td>0</td> <td>0</td> </tr> <tr> <td>4</td> <td>4</td> <td>0x0000</td> <td>0x0001</td> <td>0</td> <td>0</td> </tr> <tr> <td>5</td> <td>5</td> <td>0x0000</td> <td>0x0001</td> <td>0</td> <td>0</td> </tr> <tr> <td>6</td> <td>6</td> <td>0x0000</td> <td>0x0001</td> <td>0</td> <td>0</td> </tr> <tr> <td>7</td> <td>7</td> <td>0x0000</td> <td>0x0001</td> <td>0</td> <td>0</td> </tr> <tr> <td>8</td> <td>8</td> <td>0x0000</td> <td>0x0001</td> <td>0</td> <td>0</td> </tr> </tbody> </table>	PORTID	IFX	COFIG	STATE	LINK	SPEED	DUPLEX						1	1	0x0000	0x0001	0	0	2	2	0x0000	0x0001	0	0	3	3	0x0000	0x0001	0	0	4	4	0x0000	0x0001	0	0	5	5	0x0000	0x0001	0	0	6	6	0x0000	0x0001	0	0	7	7	0x0000	0x0001	0	0	8	8	0x0000	0x0001	0	0
PORTID	IFX	COFIG	STATE	LINK	SPEED																																																								
DUPLEX																																																													
1	1	0x0000	0x0001	0	0																																																								
2	2	0x0000	0x0001	0	0																																																								
3	3	0x0000	0x0001	0	0																																																								
4	4	0x0000	0x0001	0	0																																																								
5	5	0x0000	0x0001	0	0																																																								
6	6	0x0000	0x0001	0	0																																																								
7	7	0x0000	0x0001	0	0																																																								
8	8	0x0000	0x0001	0	0																																																								

```

    9    9    0x0000    0x0001    0    0    0
   10   10    0x0000    0x0001    0    0    0
   11   11    0x0000    0x0001    0    0    0
   12   12    0x0000    0x0001    0    0    0
   13   13    0x0000    0x0001    0    0    0
   14   14    0x0000    0x0001    0    0    0
   15   15    0x0000    0x0001    0    0    0
   16   16    0x0000    0x0001    0    0    0

QTECH#show of flowtable
openflow flow count = 1
*****FLOW
START*****
KEY:
      SMAC                                DMAC                                SIP
DIP
    08:c6:b3:56:d3:22    08:c6:b3:a3:62:13    NA                                NA
      INPORT                                VLANID                                ETYPE
VLAN_PRIORITY
      26                                NA                                NA
NA
      TCP/UDP_SPORT                                TCP/UDP_DPORT                                DSCP
IP_PROTOCOL
      NA                                NA                                NA
NA
      WILDCARD                                SIP_MASK                                DIP_MASK
      3fff2                                NA                                NA
      PRIORITY                                IDLE_TIMEOUT                                HARD_TIMEOUT
SEND_FLOW_REM
      120                                0                                0
0
-----
-----
ACTION:
ACTION_SIZE = 8
OUTPUT_PORT = 7
*****FLOW
END*****
```

Common Errors

- The controller IP address is incorrectly configured.
- The TCP port of the controller is incorrectly configured.
- You forget to configure the IP address of the local management channel.

Configuring OpenFlow STP

- Configuration Effect
- Enable the STP function on the SDN controller or the STP function on the local device, so that the SDN controller or local device performs STP processing.

Notes

- The configuration is effective only during the next connection to the controller after the OpenFlow function is enabled.

Configuration Method

- ➔ **Enabling the STP Function on the OpenFlow Device**
 - Mandatory configuration. The STP function is enabled on the SDN controller by default.
- ➔ **Enabling STP Management on the SDN Controller**
 - Default configuration.
- ➔ **Displaying Current Configuration**
 - Display the current port status.

Verification

- Display current configuration using the show of port command.

Related Commands

➔ Enabling the OpenFlow Function

Command Syntax	of controller-ip <i>ip-address</i> [port <i>port-value</i>] interface [<i>interface-id</i>]
Parameter Description	controller-ip <i>ip-address</i> : controller IP address. port <i>port-value</i> : port that connects to the controller. The default value is 6633. interface <i>interface-id</i> : port ID, which can be an out-of-band management interface or a common in-band physical Ethernet interface.
Command Mode	Global configuration mode
Usage Guide	-

➔ Disabling the OpenFlow Function

Command Syntax	no of controller-ip
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	Run this command before switching the controller.

➔ Enabling or Disabling the Local STP Function on the OpenFlow Device

Command Syntax	of stp
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	Run this command to select enabling the local STP function on the network device or enabling the STP function on the OpenFlow controller.

➔ **Displaying the Connection Status Between the OpenFlow Device and the Controller**


Command Syntax	show of
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	-

➔ **Displaying Port Information About the OpenFlow Device**

Command Syntax	show of port
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	-

Configuration Examples

➔ **Enabling Local STP or STP of OpenFlow**

Network Environment Figure 16-4	
Configuration Method	<ul style="list-style-type: none"> ● Enable STP of OpenFlow. <code>QTECH(config)#of stp</code> ● Enable local STP. <code>QTECH(config)#no of stp</code>

Verification

- Display STP status of the OpenFlow device.

```
QTECH(config)#of stp
QTECH(config)#show of port
STP is controlled by SDN Controller.
```

- Display local STP status.

```
QTECH(config)#no of stp
QTECH(config)#show of port
STP is controlled by local device.
```

16.5. Monitoring and Maintaining

Clearing Various Information

-

Displaying the Running Status

Command	Function
show of	Displays the status of the current connection between the OpenFlow device and the controller
show of port	Displays the port status of the current OpenFlow device
show of flowtable	Displays the flow table of the current OpenFlow device

Displaying Debugging Information