QTECH
МИР ДОСТУПНЕЕ

System Configuration

www.qtech.ru

Оглавление

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

1.1.2. 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

Deployment

```
Remarks
A is the network device to be managed.
```

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.

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.

1.1.2 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.

1.2.2. 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.
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.	Use this configuration mode to configure various interfaces of the network device.

			When using the interface command, you must specify the interface.	
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.

1.2.3. 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

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

For example

1.2.4. Abbreviated Commands

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

```
QTECH(config)#int g0/1

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

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)#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:

Full help is available when you are ready to enter a
```

```
   command argument (e.g. 'show ?') and describes each possible

   argument.

Partial help is provided when an abbreviated argument is entered

   and you want to know what arguments match the input

   (e.g. 'show pr?'.)
```

1.2.5. 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.

1.2.6. 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.

1.2.7. 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.

1.2.8. 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 ($).

The default screen width is 80 characters.

1.2.9. 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* | [**regexp**] **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* | [**regexp**] **exclude** *regular-expression*	Filters the output of the **show** command. Except those containing the specified contents, all lines will be output.
show *any-command* | [**regexp**] **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
QTECH#show running-config | regexp include GigabitEthernet [0-9]/1 interface GigabitEthernet 0/1
QTECH#
```

1.2.10. Command Alias

You can configure any word as the alias of a command to simply 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 0.0.0.0192.1.1.1* 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.

These default aliases cannot be deleted.

❖ **Configuring a Command Alias**

Command	**alias *mode command-alias original-command***
Parameter Description	*mode*: indicates the command mode of the command represented by the alias. *command-alias*: indicates the command alias. *original-command*: 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 ip route *0.0.0.0 0.0.0.0 192.168.1.1.***
	QTECH#configure terminal QTECH(config)#alias config ir ip route 0.0.0.0 0.0.0.0 192.168.1.1
Verification	Run the **show alias** command to check whether the alias is configured successfully.
	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
	Use the configured alias to run the command, and run the show running-config command to check whether the alias is configured successfully.

	QTECH(config)#ir QTECH(config)#show running-config Building configuration… ! 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

Configuration Steps	**In global configuration mode, configure the alias "ir" to represent the front part "ip route" of the default route configuration command.**
	QTECH#configure terminal QTECH(config)#alias config ir ip route
Verification	Run the **show alias** command to check whether the alias is configured successfully.

	QTECH(config)#show alias Exec mode alias: h help p ping
	s show u undebug un undebug Global configuration mode alias: ir ip route
	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.
	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 ! 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.

2.1. 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
User Access Control	Controls the terminal access to network devices on the internet based on passwords and privileges.
Login Authentication Control	Performs username-password authentication to grant access to network devices when AAA is enabled. (Authentication is performed by a dedicated server.)
Basic System Parameters	Refer to the parameters of a system, such as the clock, banner, and Console baud rate.
Displaying Configurations	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).
Multiple-configuration Booting	Allows users to modify the path for saving startup configurations of the device and the corresponding file name.
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.
Running Batch File Commands	Runs the commands in batches.

2.2. 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.

❖ 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.

To enable level increase logging, run the **login privilege log** command.

❖ 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. 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 Non-AAA Authentication for Line-Based Login When AAA Is Enabled

Run the **login access non-aaa** command in global configuration mode.

Perform this configuration on every device.

❖ 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.

2.4. 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.

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, 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.

The **startup-config** file copied to the device only supports the UTF-8 (no BOM) format.

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.

2.5. Multiple-configuration Booting

Multiple-configuration booting allows users to modify the path for saving startup configurations of the device and the corresponding file name. At present, configurations can be saved to an extended flash memory and an extended USB flash drive of a device. To save configurations in an extended USB flash drive, the device must support at least one USB interface. If the device supports two or more USB interfaces, startup configurations are saved in **/mnt/usb0**.

Working Principle

By default, the startup configuration file of a device is saved in **Flash:/config.text** and named **config.text**. Use this command to modify the path for saving startup configurations of the device and the corresponding file name.

The startup configuration file name follows a slash "/", for example, **Flash:/QTECH.text** and **Usb0:/QTECH.text**

⚠The startup configuration file name consists of a path and a file name. The path is mandatory. Otherwise, configurations cannot be saved by using the **write** command. Take **Flash:/QTECH/QTECH.text** and

Usb0:/QTECH/QTECH.text as examples, where the **Flash:/QTECH** and **Usb0:/QTECH** folders must exist. In master-slave mode, all device paths are required.

⚠To save the startup configuration file to a USB flash drive, the device must provide a USB interface with a USB flash drive inserted. Otherwise, configurations cannot be saved by using the **write** command. In master-slave

mode, all devices must have USB flash drives connected.

❖ Related Configuration

Modifying the Path for Saving Startup Configurations and the Corresponding File Name

Run the **boot config { flash:***filename* | **usb0:***filename* **}** command to modify the path for saving startup configurations and the corresponding file name.

❖ Displaying the Path for Saving Startup Configurations and the Corresponding File Name

Run the **show boot config** command to display the path for saving startup configurations and the corresponding file name.

❖ Telnet

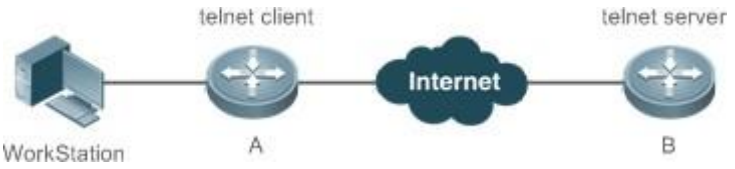
Working Principle

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.

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.

Running Batch File Commands

In system management, sometimes it takes a long time to enter many commands on the CLI to manage a function. This process is prone to errors and omissions. You can put the commands to a batch file according to configuration steps and execute the file to complete related configuration.

ℹ You can specify the name and content of the batch file on your PC and transfer the file to the device flash memory through TFTP. The batch processing content simulates user input. Therefore, you need to edit the batch file content

according to the CLI command configuration sequence. In addition, you need to write the responses to interactive commands to the batch file to ensure normal command execution.

⚠ The batch file size must not exceed 128 KB; otherwise, it will fail to be executed. You can divide a large batch file into multiple parts not larger than 128 KB each.

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.

Character Set Encoding

The character set encoding function enables the device to specify a unified character set encoding format. After a client enters a command in the CLI, the command is automatically converted into a command in the unified character set encoding format before delivery.

ℹ When current running configurations in different formats exist on a device, you can set a unified character set encoding format only after manually delete running configurations that are not in the unified character set encoding format.

Related Configuration

❖ Setting the Character Set Encoding Format

Run the **language character-set { UTF-8 | GBK | default }** command to set the character set encoding format.

The value **default** indicates that mixed codes are supported.

❖ Displaying the Character Set Encoding Format

Run the **show language character-set** command to display the current character set encoding format.

Configuration

Configuring Passwords and Privileges	(Optional) It is used to configure passwords and command privilege levels.	
	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	(Optional) It is used to configure different login modes and authentication methods.	
	username	Configures local user account information and optional authorization information.
	login local	Configures local authentication for

		line-based login.
	login access non-aaa	Configures non-AAA authentication for line-based login when AAA is enabled.
	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.
Configuring Multiple-configuration Booting	(Optional) It is used to modify the startup configuration file.	
	boot config { **flash:***filename* | **usb0:***filename* }	Modifies the path for saving startup configurations and the corresponding file name.
Configuring a Restart Policy	(Optional) It is used to configure a system restart policy.	
	reload	Restarts a device.
Running Batch File Commands	(Optional) It is used to run the commands in batches.	
	execute { [**flash:**] *filename* }	Runs the commands in batches.
Configuring Language Character Set	(Optional) It is used to configure the language character set.	
	language character-set { **UTF-8** | **GBK** | **default** }	Configures the language character set.

2.6. 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	*level*: Indicates a specific user level. *password:* Indicates the password used to enter privileged EXEC mode. *0:* Indicates that the password is entered in plaintext. *7:* Indicates that the password is entered in cyphertext. *encrypted-password:* 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	*level*: Indicates a specific user level. secret: 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. *encrypted-password*: 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	*privilege-level*: 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	*privilege-level*: 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 *privilege-level* is specified, the current privilege level is reduced to the specified level.

	privilege-level 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 **}** ***command-string***
Parameter Description	*mode*: 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. *command-string*: 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 command* command in global configuration mode.

❖ Specifying a Line Password

Command	Password **[** 0 **|** 7 **]** ***line***
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	login
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	Assign privilege level 1 to the **reload** command and its subcommands.
	QTECH# configure terminal QTECH(config)# privilege exec all level 1 reload QTECH(config)# enable secret level 1 0 test QTECH(config)# end

Verification	Check whether the **reload** command and its subcommands are accessible at level 1.
	QTEC H# disabl e 1 QTEC H> reload ? at reload at<cr>

2.7. 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.

❖ Configuring Non-AAA Authentication for Line-Based Login When AAA Is Enabled

Optional.

Run the **login access non-aaa** command in global configuration mode to authenticate line-based login in non-AAA mode 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	username ***name*** **[** login mode **{** aux **|** 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*** **|** secret **[** 0 **|** 5 **]** ***text-string***

Parameter Description	*name*: Indicates a user name. **login mode**: Indicates the login mode. **aux**: Sets the login mode to AUX. **console**: Sets the login mode to Console. **ssh**: Sets the login mode to SSH. **telnet**: Sets the login mode to Telnet. **online amount** *number*: Indicates the maximum number of online accounts. **permission** *oper-mode path*: Configures the file operation permission. *op-mode* indicates the operation mode, and *path* indicates the directory or path of a specific file. **privilege** *privilege-level*: Indicates the account privilege level, ranging from 0 to 15. **reject remote-login**: Rejects remote login by using the account. **web-auth**: Allows only Web authentication for the account. **pwd-modify**: Allows the account owner to change the password. This option is available only when **web-auth** is configured. **nopassword**: Indicates that no password is configured for the account. **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. **secret** [**0** | **5**] *text-string*: Indicates the password configured for the account. 0 indicates that the password is input in plaintext, and 5 indicates that the password is input in cyphertext. The default is plaintext.

Command Mode	Global configuration mode
Usage Guide	Use this command to create a local user database to be used by authentication. If the value 7 is selected for the encryption type, the entered cyphertext string must consist of an even number of characters. This setting is applicable to the scenario where encrypted passwords may be copied and pasted. In other cases, the value 7 is not selected.

❖ Configuring Local Authentication for Line-Based Login

Command	login local
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 **username** command.

❖ Configuring AAA Authentication for Line-Based Login

Command	login authentication **{** default **|** ***list-name*** **}**
Parameter Description	**default:** Indicates the default authentication method list name. *list-name*: Indicates the optional method list name.
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.

❖ Configuring Non-AAA Authentication for Line-Based Login When AAA Is Enabled

Command	login access non-aaa
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command when you need to perform non-AAA authentication on line-based login in the case that AAA is enabled. The configuration takes effect for all terminals.

❖ Enabling the Telnet Client Service

Command	telnet **[** oob **]** ***host*** **[** ***port*** **]** **[** /source **{** ip ***A.B.C.D*** | ipv6 ***X:X:X:X::X*** | interface ***interface-name }*** **]** **[** /vrf ***vrf-name*** **]**
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** *interface-name*: Indicates the source port used by the Telnet client. **/vrf** *vrf-name*: Indicates the name of the virtual routing and forwarding (VRF) table to be queried.
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 ***session-id***
Parameter Description	*session-id*: 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 ***minutes*** **[** ***seconds*** **]**
Parameter Description	*minutes*: Indicates the connection timeout time in the unit of minutes. *seconds*: 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 ***minutes*****[** output **]**
Parameter Description	*minutes*: 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	• **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.** • **Run the** telnet **command in privileged EXEC mode, and run the** do telnet **command in privileged EXEC mode/configuration mode/interface configuration mode.**
	QTECH# telnet 192.168.65. 119 Trying 192.168.65. 119 ..... Open User Access Verification Password:

	QTECH# telnet 2AAA:BBBB ::CCCC Trying 2AAA:BBBB ::CCCC.....Open User Access Verification Password:
Verification	Check whether the Telnet sessions are established to the remote network devices.

❖ Configuring the Connection Timeout Time

Configuration Steps	**Set the connection timeout time to 20 minutes.**
	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.
Verification	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	**Set the session timeout time to 20 minutes.**

Steps	
	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.
Verification	Check whether the session between a terminal and the local device is disconnected when no input is detected during the timeout time.

2.8. 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	*hh:mm:ss*: Indicates the current time, in the format of *hour* (24-hour format):*minute*:*second*. *day*: Indicates a day (1–31) of the month. *month*: Indicates a month (from January to December) of the year. *year*: 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	Privileged EXEC mode

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 ***name***
Parameter Description	*name*: 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 ***string***
Parameter Description	*string*: 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	*speed*: 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	▪ **Change the system time to 2003-6-20, 10:10:12.**
	QTECH# clock set 10:10:12 6 20 2003 //Configure the system time and date.
Verification	Run the **show clock** command in privileged EXEC mode to display the system time.
	QTECH# show clock //Confirm that the changed system time takes effect. clock: 2003-6-20 10:10:54

❖ Configuring Daily Notification

Configuration Steps	**Configure the daily notification message "Notice: system will shutdown on July 6th." with the pound key (#) as the delimiter.**
	QTECH(config)# banner motd #//Starting delimiter Enter TEXT message. End with the character '#'. Notice: system will shutdown on July 6th.# //Ending delimiter QTECH(config)#
Verification	• 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.
	C:\>telnet 192.168.65.236 Notice: system will shutdown on July 6th. Access for authorized users only. Please enter your password. User

	Access Verificatio n Password:

❖ Configuring a Login Banner

Configuration Steps	▪ **Configure the login banner message "Access for authorized users only. Please enter your password." with the pound key (#) as the delimiter.**
	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)#
Verification	▪ Run the **show running-config** 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.
	C:\>telnet 192.168.65.236 Notice: system will shutdown on July 6th. Access for authorized users only. Please enter your password. User Access Verificatio n Password:

❖ Configuring the Serial Port Baud Rate

Configuration Steps	**Set the serial port baud rate to 57,600 bps.**
	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.
Verification	▪ Run the **show** command to display the configuration.
	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
Configuration Steps	Set the serial port baud rate to 57,600 bps.
	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.
Verification	Run the **show** command to display the configuration.

	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

2.9. 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 **|** web-server **[** http	https	all **] |** 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. **web-server** [**http	https	all**]: Enables or disables the Web 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	▪ **Enable the SSH Server service.**
	QTECH# configure terminal //Enter global configuration mode. QTECH(config)#enable service ssh-server //Enable the SSH Server service.
Verification	▪ 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.

2.10. Configuring Multiple-configuration Booting

Configuration Effect

Modify the path for saving startup configurations and the corresponding file name.

Notes

The startup configuration file name consists of a path and a file name. The path is mandatory. Otherwise, configurations cannot be saved by using the write command. Take Flash:/QTECH/QTECH.text and Usb0:/QTECH/QTECH.text as examples, where the Flash:/QTECH and Usb0:/QTECH folders must exist. In master-slave mode, all device paths are required.

To save the startup configuration file to a USB flash drive, the device must provide a USB interface with a USB flash drive inserted. Otherwise, configurations cannot be saved by using the **write** command. In master-slave mode, all devices must have USB flash drives connected.

Configuration Steps

❖ Modifying the Path for Saving Startup Configurations and the Corresponding File Name

(Optional) Perform this configuration when you need to modify the startup configuration file.

Verification

- Run the **show boot config** command to display the path for saving startup configurations and the corresponding file name.

Related Commands

- Modifying the Path for Saving Startup Configurations and the Corresponding File Name

Command	boot config **{** flash:***filename*** **|** usb0:***filename*** **}**
Parameter Description	**flash:** Saves the startup configuration file in the extensible Flash. **usb0:** Saves the startup configuration file in USB0 device. The device must have a USB interface into which a USB flash drive is inserted.
Command Mode	Global configuration mode
Usage Guide	Use this command to modify the path for saving startup configurations and the corresponding file name.

Configuration Example

❖ Changing the Path of the Startup Configuration File to Flash:/QTECH.text

Configuration Steps	▪ **Change the startup configuration file path into Flash:/QTECH.text.**
	QTECH# configure terminal //Enter global configuration mode. QTECH(config)# boot config flash:/QTECH.text//Change the path and file name into flash:/QTECH.text.
Verification	▪ Run the **show boot config** command to display the path for saving startup configurations and the corresponding file name.

2.11. 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

If you configure a specific time, the system will restart at the time. The time must be a time in the future. The **month day year**

parameter is optional. If it is not specified, the system clock time is used by default.

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 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.)

Related Commands

- ❖ Restarting a Device

Command	reload **[** at **{** ***hh*** **[** ***:mm*** **[** ***:ss*** **]] } [** ***month*** **[** ***day*** **[** ***year*** **]]]]**
Parameter Description	**at** *hh:mm:ss*: Indicates the time when the system will restart. *month*: Indicates a month of the year, ranging from 1 to 12. *day*: Indicates a date, ranging from 1 to 31. *year*: Indicates a year, ranging from 1993 to 2035. Abbreviation is not supported.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to enable a device to restart at a specific time.

2.12. Running Batch File Commands

Configuration Effect

- Run the commands in batches.

Configuration Steps

- Running the execute Command

Run the **execute** command, with the path set to the batch file to be executed.

You can specify the name and content of the batch file on your PC and transfer the file to the device flash memory through TFTP. The batch processing content simulates user input. Therefore, you need to edit the batch file content

according to the CLI command configuration sequence. In addition, you need to write the responses to interactive commands to the batch file to ensure normal command execution.

The batch file size must not exceed 128 KB; otherwise, it will fail to be executed. You can divide a large batch file into multiple parts not larger than 128 KB each.

Related Commands

Command	execute **{ [** flash: **]** ***filename*** **}**
Parameter Description	*filename*: Indicates the path for the batch file to be executed.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to run the commands related to a function in batches.

2.13. Configuring the Character Set Encoding Format

Configuration Effect

A unified character set encoding format is used on a device.

Notes

None

Configuration Steps

- Setting a Character Set Encoding Format

Run the **language character-set** command to set a character set encoding format.

When current running configurations in different formats exist on a device, you can set a unified character set encoding format only after manually delete running configurations that are not in the unified character set encoding format.

Verification

Run the **show language character-set** command to display the specified character set encoding format.

Related Commands

Command	language character-set **{** UTF-8 **|** GBK **|** default **}**
Parameter Description	**UTF-8**: Sets the character set encoding format to UTF-8. **GBK**: Sets the character set encoding format to GBK. **default**: Sets the character set encoding format to the default format (mixed codes supported).
Command Mode	Global configuration mode
Usage Guide	Run this command to use a unified character set encoding format on a device.

Common Errors

N/A

Monitoring

Displaying

Description	Command
show boot config	Displays the save path and file name.
show clock	Displays the current system time.
show line { **aux** *line-num* | **console** *line-num* | **tty** *line-num* | **vty** *line-num* **|** *line-num* }	**show line** { **aux** *line-num* | **console** *line-num* | **tty** *line-num* | **vty** *line-num* **|** *line-num* }
show reload	Displays system restart settings.
show running-config [**interface**	Displays the current running configurations of the device or the

interface]	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.
show language character-set	Displays the language character set.

3.1. Overview

There are various types of terminal ines 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.

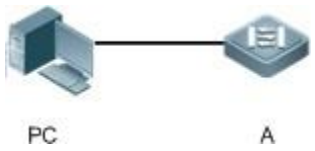
3.2. Applications

Application	Description
Accessing Consolea Device Through	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.

3.2.1. Accessing a Device Through Console

Scenario

Figure 3-1



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

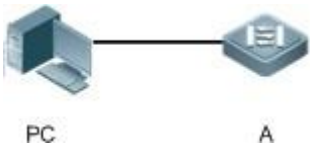
Deployment

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.

3.2.2. 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

<table>
<tr><th>Configuration</th><th colspan="2">Description and Command</th></tr>
<tr><td rowspan="3">Entering Line Configuration Mode</td><td colspan="2">(Mandatory) It is used to enter the line configuration mode.</td></tr>
<tr><td>line [console | vty] first-line [last-line]</td><td>Enters the specified line configuration mode.</td></tr>
<tr><td>line vty line-number</td><td>Increases or reduces the number of available VTY lines.</td></tr>
</table>

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

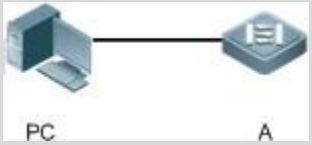
Command	line [console | vty] ***first-line*** [***last-line***]
Parameter Description	**console**: Indicates the Console port. **vty**: Indicates a virtual terminal line, which supports Telnet or SSH. *first-line*: Indicates the number of the first line. *last-line*: Indicates the number of the last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

❖ Increasing/Reducing the Number of VTY Lines

Command	line vty ***line-number***
Parameter Description	*line-number*: 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.

Configuration Example

Scenario Figure 3-3	
Configuration Steps	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. Run the **show line console** 0 command to display the status of the Console line. Enter global configuration mode and run the **line vty** command to increase the number of VTY terminals to 36.
A	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
Verification	After running the **show line** 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* }
Displays historical records of a line.	**show history**
Displays the privilege level of a line.	**show privilege**
Displays users on a line.	**show user** [**all**]

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

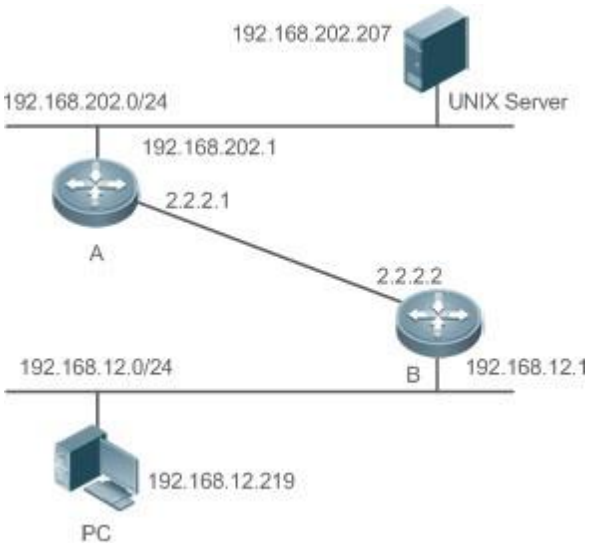
Typical Application	Scenario
Applying Time Range to an ACL	Apply a time range to an ACL module so that the time-based ACL takes effect

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
Using Absolute Time Range	Sets an absolute time range for a time-based application, so that a certain function takes effect within the absolute time range.
Using Periodic Time	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.

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.

4.4. Configuration Details

Configuration Item	Suggestions and Related Commands	
Configuring Time Range	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 ***time-range-name***
Parameter Description	*time-range-name*: name of the time range to be created.
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 ***time date*** **] | [** end ***time date*** **] }**
Parameter Description	**start** *time date*: start time of the range. **end** *time date*: 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 ***day-of-the-week time*** to **[*day-of-the-week*] *time***
Parameter Description	*day-of-the-week*: the week day when the periodic time starts or ends *time*: 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. If you want to change the periodic time, it is recommended to disassociate the time range first and associate the time range after the periodic time is changed.

4.5. Monitoring

Displaying the Running Status

Function	Command
Displays time range configuration.	**show time-range** [*time-range-name*]

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. Applications

Application	Description
HTTP Application Service	Users manage devices based on Web.
Remote HTTP Upgrade Service	The HTTP upgrade function is used to upgrade files.

5.2.1. HTTP Application Service

Scenario

After the HTTP service is enabled, users can access the Web management page after passing authentication by only entering **http://IP address of a device** in the browser of a PC. On the Web page, users you can monitor the device status, configure devices, upload and download files.

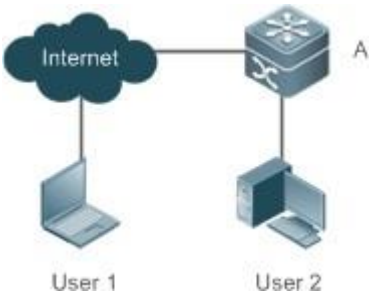
Take the following figure as an example to describe Web management.

Users can remotely access devices on the Internet or configure and manage devices on the Local Area Network (LAN) by logging in to the Web server.

According to actual conditions, users can choose to enable the HTTPS or HTTP service or enable the HTTPS and HTTP services at the same time.

Users can also access the HTTP service of devices by setting and using HTTP/1.0 or HTTP/1.1 in the browser.

Figure 5-1



Remarks	**A is a QTECH device.** **User 1 accesses the device through the Internet. User 2 accesses the device through a LAN.**

Deployment

- When a device runs HTTP, users can access the device by entering **http://IP address of the device** in the browser of a PC.
- When a device runs HTTPS, users can access the device by entering **https://IP address of the device** in the browser of a PC.

5.2.2. Remote HTTP Upgrade Service

Scenario

HTTP remote upgrade means that a device is connected to a remote HTTP server as a client and realizes local file upgrade by obtaining files from the server. The default domain name of a Web server provided by QTECH is **rgos.QTECH.com.cn**.

Take the following figure as an example. Use the HTTP remote upgrade function to upgrade files.

A device obtains upgrade files from a QTECH server every day on a scheduled basis.

Download the latest files from the server and update the upgrade device. Figure 5-2

Remarks	A is a QTECH device. User is a PC user. Web server is a QTECH server.

Deployment

When a device runs HTTP, directly send a command to the device through the browser and obtain the latest upgrade files from the Web server.

5.3. Features

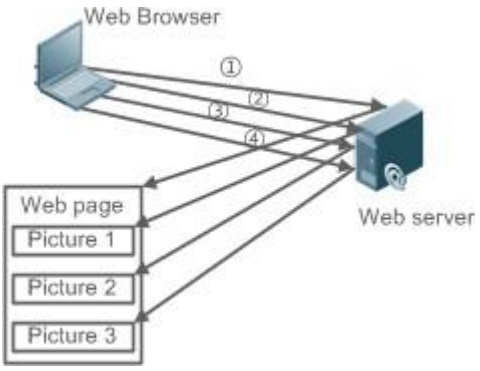
Basic Concepts

❖ 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 my 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 5-2



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 5-3

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

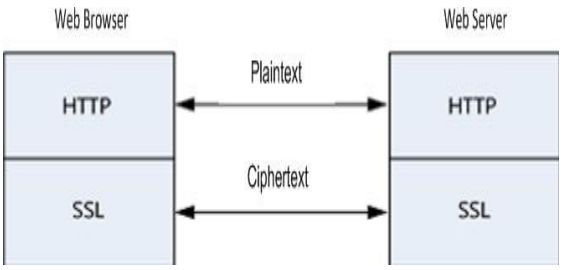
Which HTTP version will be used by a device is decided by the Web browser.

❖ 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 5-4



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
HTTP Service	Users log in to devices through Web pages to configure and manage devices.
Local HTTP Upgrade Service	Upgrade files are uploaded to a device to realize file upgrade on the device.

5.3.1. HTTP Service

HTTP is a service provided for Web management. Users log in to devices through Web pages to configure and manage devices.

Working Principle

Web management covers Web clients and Web servers. Similarly, the HTTP service also adopts the client/server mode. The HTTP client is embedded in the Web browser of the Web management client. It can send HTTP packets and receive HTTP response packets. The Web server (namely HTTP server) is embedded in devices. The information exchange between the client and the server is as follows:

- A TCP connection is established between the client and the server. The default port ID of the HTTP service is 80 and the default port ID of the HTTPS service is 443.
- The client sends a request message to the server.
- The server resolves the request message sent by the client. The request content includes obtaining a Web page, executing a CLI command, and uploading a file.
- After executing the request content, the server sends a response message to the client.

Related Configuration

❖ Enabling the HTTP Service

By default, the HTTP service is disabled.

The **enable service web-server** command can be used to enable HTTP service functions, including the HTTP service and HTTPS service.

The HTTP service must be enabled so that users can log in to devices through Web pages to configure and manage devices.

❖ Configuring HTTP Authentication Information

By default, the system creates the **admin** account. The account cannot be deleted and only the password of the account can be changed. The administrator account is the admin account, which corresponds to the level 0 permission. The administrator account owns all permissions on the Web client and can edit other management accounts and authorize the accounts to access pages. The new accounts that are added correspond to the level 1 permission.

The **webmaster level** command can be used to configure an authenticated user name and a password.

After this command is run, you need to enter the configured user name and password to log in to the Web page.

❖ Configuring an HTTP Service Port

By default, the HTTP service port ID is 80.

The **http port** command can be used to configure an HTTP service port ID. The value range of the port ID is 80 and 1025 to 65535.

By configuring an HTTP service port ID, you can reduce the number of attacks initiated by illegal users on the HTTP service.

❖ Configuring an HTTPS Service Port

By default, the HTTPS service port ID is 443.

The **http secure-port** command can be used to configure an HTTPS service port ID. The value range of the port ID is 443 and 1025 to 65535.

By configuring an HTTPS service port ID, you can reduce the number of attacks initiated by illegal users on the HTTPS service.

5.3.2. Remote HTTP Upgrade Service

A device is connected to a remote HTTP server as a client and realizes local file upgrade by obtaining files from the server.

Working Principle

- The server is connected. When the server is connected, the server address configured by the user is connected in preference. If the server address cannot be connected, the server addresses in the local upgrade files are connected in turn.
- The versions of service modules of the local device are sent to the server.
- The server resolves the versions and provides a file download list.

- Based on the file download list, the device is connected to the file server and downloads upgrade files. Different downloaded files can be used to connect different servers.
- The device upgrades files.

Related Configuration

❖ Configuring an Upgrade Server Address

By default, the server address is the official website of QTECH, namely **rgos.QTECH.com.cn**.

The **http update server** command can be used to configure the address and port ID of a remote HTTP upgrade server. If you specify the server, you need to contact QTECH R&D personnel to help create an upgrade server and obtain the latest version of service modules in real time. You are advised not to configure an upgrade server but use the default QTECH official website for upgrade. The upgrade server on QTECH official website is maintained by dedicated R&D personnel.

During an HTTP upgrade, the server address configured by using the command is connected in preference. If the server address cannot be connected, server addresses recorded locally are connected in turn. If none of the server addresses can be connected, the upgrade cannot be performed.

❖ Configuring an HTTP Upgrade Mode

By default, HTTP uses the automatic upgrade mode.

The **http update mode** command can be used to set the HTTP upgrade mode to manual upgrade.

❖ Configuring the HTTP Automatic Upgrade Time

By default, the remote automatic HTTP upgrade time is random.

The **http update time** command can be used to change the automatic upgrade time. Only a time point in each day can be configured and the precision reaches minute.

After this command is run, if the upgrade mode is automatic upgrade, the device detects and upgrades files on the server at the configured time every day.

❖ Configuring Upgrade through the Management Port

By default, an HTTP upgrade is performed through a common port. Certain devices support the management port. The **http update set oob** command can be used to perform an upgrade on devices through the management port.

❖ Detecting Upgrade Files on the HTTP Server

By default, the function of detecting HTTP upgrade files is disabled.

The **http check-version** command can be used to detect upgrade files on the HTTP server. This command can be run to detect the latest files on the server.

❖ Manually Upgrading Files

Run the **http update** command to manually upgrade files.

5.4. Configuration

Configuration	Description and Command	
Configuring the HTTP Service	(Mandatory) It is used to enable the HTTP service.	
	enable service web-server	Enables the HTTP service.
	webmaster level	Configures HTTP authentication information.
	http port	Configures an HTTP service port.
	http secure-port	Configures an HTTPS service port.
Configuring a Remote HTTP Upgrade		
	⚠ (Mandatory) It is used to realize a remote HTTP upgrade.	
	http update server	Configures an HTTP upgrade server.
	http update mode	Configures an HTTP upgrade mode.
	http update time	Configures the HTTP automatic upgrade time.
	http update set oob	Configures upgrade through t management port.
	http check-version	Detects upgrade files on an

		HTTP server.
	http update	Manually upgrades files.

5.4.1. Configuring the HTTP Service

Configuration Effect

After the HTTP service is enabled on a device, users can log in to the Web management page after passing authentication and monitor the device status, configure devices, upload and download files.

Configuration Steps

❖ Enabling the HTTP Service

Mandatory

If there is no special requirement, enable the HTTP service on QTECH devices. Otherwise, the Web service is inaccessible.

❖ Configuring HTTP Authentication Information

By default, the user name **admin** and the password **admin** are configured.

If there is no special requirement, you can log in to the Web page by using the default user name and directly update authentication information through the Web browser. If you always use the default account, security risks may exist because unauthorized personnel can obtain device configuration information once the IP address is disclosed.

❖ Configuring an HTTP Service Port

If an HTTP service port needs to be changed, the HTTP service port must be configured.

If there is no special requirement, the default HTTP service port 80 can be used for access.

❖ Configuring an HTTPS Service Port

If an HTTPS service port needs to be changed, the HTTPS service port must be configured.

If there is no special requirement, the default HTTPS service port 443 can be used for access.

Verification

Enter **http://IP address of the device: service port** to check whether the browser skips to the authentication page.

Enter **https://IP address of the device: service port** to check whether the browser skips to the authentication page.

Related Commands

❖ Enabling the HTTP Service

Command	enable service web-server **[** http **|** https **|** all **]**
Parameter Description	**http**	**https**	**all**: Enables the corresponding service. **http** indicates enabling the HTTP service, **https** indicates enabling the HTTPS service, and **all** indicates enabling the HTTP and HTTPS services at the same time. By default, the HTTP and HTTPS services are enabled at the same time.
Command Mode	Global configuration mode.
Usage Guide	If no key word or **all** is put at the end of the command when the command is run, the HTTP and HTTPS services are enabled at the same time. If the key word **http** is put at the end of the command, only the HTTP service is enabled; if the key word **https** is put at the end of the command, only the HTTPS service is enabled. The **no enable service web-server** or **default enable service web-server** command is used to disable the corresponding HTTP service. If no key word is put at the end of the **no enable service web-server** or **default enable service web-server** command, the HTTP and HTTPS services are disabled.

❖ Configuring HTTP Authentication Information.

Command	webmaster level ***privilege-level*** username ***name*** password **{** ***password*** **|** **[** 0	7 **]** ***encrypted-password*** **}**
Parameter Description	*privilege-level*: Permission level bound to a user. *name*: User name. *password*: User password. **0	7**: Password encryption type. 0: no encryption; 7: simple encryption. The default value is **0**. *encrypted-password*: Password text.
Command Mode	Global configuration mode.

Usage Guide	When the HTTP server is used, you need to be authenticated before logging in to the Web page. The **webmaster level** command is used to configure a user name and a password for logging in to the Web page. Run the **no webmaster level** *privilege-level* command to delete all user names and passwords of the specified permission level. Run the **no webmaster level** *privilege-level* **username** *name* command to delete the specified user name and password. User names and passwords involve three permission levels: Up to 10 user names and passwords can be configured for each permission level. By default, the system creates the **admin** account. The account cannot be deleted and only the password of the account can be changed. The administrator account is the **admin** account, which
	corresponds to the level 0 permission. The administrator account owns all permissions on the Web client and can edit other management accounts and authorize the accounts to access pages. The new accounts that are added correspond to the level 1 permission.

❖ Configuring an HTTP Service Port

Command	http port ***port-number***
Parameter Description	*port-number*: Configures an HTTP service port. The value range is 80 and 1025 to 65535.
Command Mode	Global configuration mode.
Usage Guide	Run the command to set an HTTP service port.

❖ Configuring an HTTPS Service Port

Command	http secure-port ***port-number***
Parameter Description	*port-number*: Configures an HTTPS service port. The value range is 443 and 1025 to 65535.

Command Mode	Global configuration mode.
Usage Guide	Run the command to set an HTTPS service port.

Configuration Example

❖ Managing one QTECH Device by Using Web and Logging in to the Device through a Web Browser to Configure Related Functions

Log in to the device by using the **admin** account configured by default.

To improve security, the Web browser is required to support both HTTP and HTTPS for access.

The user is required to configure an HTTP service port to reduce the number of attacks initiated by illegal users on HTTP.

Scenario Figure 5-5	
Configuration Steps	• Enable the HTTP and HTTPS services at the same time. • Set the HTTP service port ID to 8080 and the HTTPS service port ID to 4430.
A	A#configure terminal A(config)# enable service web-server A(config)# http port 8080
	A(config)# http secure-port 4430
Verification	Check HTTP configurations.
A	A# show web- server status http server status: enabled http

	server port: 8080 https server status:enabled https server port: 4430

Common Errors

If the HTTP service port is not the default port 80 or 443, you must enter a specific configured service port in the browser. Otherwise, you cannot access devices on the Web client.

5.4.2. Configuring a Remote HTTP Upgrade

Configuration Effect

A device is connected to a remote HTTP server as a client and realizes local file upgrade by obtaining files from the server.

Notes

Before configuring the domain name of an HTTP upgrade server, enable the Domain Name System (DNS) on the device and configure the DNS address. Otherwise, the device cannot communicate with QTECH official website.

Configuration Steps

❖ Configuring the HTTP Upgrade Server

To change the server address and port ID for an HTTP remote upgrade, you must configure the HTTP upgrade server and contact QTECH R&D personnel for help.

If there is not special requirement, the upgrade server does not need to be configured and the default address can be used. The device communicates with QTECH official website and automatically obtains the latest versions of service modules. The upgrade server on QTECH official website is maintained by dedicated personnel.

❖ Configuring an HTTP Upgrade Mode

If you require the HTTP manual upgrade mode, you must configure it.

If there is no special requirement, the HTTP upgrade mode is automatic upgrade by default.

❖ Configuring the HTTP Automatic Upgrade Time

To change the HTTP automatic upgrade time, you must configure the upgrade time.

If there is not special requirement, the upgrade time does not need to be configured. The device automatically detects versions at random time. If you need to configure the upgrade time, you are advised to set the upgrade time to a time point early in the morning to avoid occupation of device traffic in rush hours.

❖ Configuring Upgrade through the Management Port

If an upgrade needs to be performed through the management port, you must configure the upgrade.

By default, an upgrade is performed through a common port by default. If an upgrade is performed through the management port, run the command to configure the upgrade. Otherwise, the upgrade fails.

❖ Detecting Upgrade Files on the HTTP Server

If upgrade files on the HTTP server need to be detected, you must perform the configuration.

If there is not special requirement, the configuration does not need to be performed because an upgrade is performed automatically.

❖ Manually Upgrading Files

Mandatory

If there is no special requirement, configure a manual upgrade file on each device.

Verification

Run the **ping** command to verify that the device can be connected to the server.

Run the **http check-version** command to obtain versions of related files on the device.

Related Commands

❖ Configuring the HTTP Upgrade Server

Command	http update server **{** ***host-name*** **|** ***ip-address*** **}** **[** port ***port-number*** **]**
Parameter Description	*host-name*: Domain name of the server. *ip-address*: Server address. **port** *port-number*: Server port ID. The value range is 1 to 65535 and the default value is 80.
Command Mode	Global configuration mode.

Usage Guide	Run this command to configure the server address and port ID for HTTP upgrade. During an HTTP upgrade, connect the server address configured by running this command. If the server address cannot be connected, connect server addresses recorded locally in turn. If none of the servers can be connected, the upgrade cannot be performed. The system records the address or addresses of one or more upgrade servers. These addresses cannot be
	modified. The server address may not be configured because the local upgrade file records addresses of possible upgrade servers. By default, the DNS needs to be enabled on a device and the DNS address needs to be configured. A server address cannot be set to an IPv6 address.

- **Configuring an HTTP Upgrade Mode**

Command	http update mode manual
Parameter Description	**manual**: Manual upgrade mode.
Configuration mode	Global configuration mode.
Usage Guide	Run the command to configure an HTTP upgrade mode. Run the command to set the HTTP upgrade mode to manual mode. After the **no http update mode manual** command is run, the HTTP upgrade mode is set to automatic mode. When it is time for automatic upgrade, the system detects upgrade files on the server and automatically downloads and upgrades the files.

❖ Configuring the HTTP Automatic Upgrade Time

Command	http update time daily ***hh*:*mm***
Parameter Description	*hh*:*mm*: Specific upgrade time in the format of hour:minute (24-hour system).
Configuration mode	Global configuration mode.
Usage Guide	Run this command to configure the automatic HTTP upgrade time. Devices are connected to the Web server (rgos.QTECH.com.cn) at the fixed time every day to detect possible upgrade files. You can view obtained files on the Web page. After the **no http update time daily** command is run, the device upgrade time is random.

❖ Configuring Upgrade through the Management Port

Command	http update set oob
Parameter Description	N/A
Configuration mode	Global configuration mode.
Usage Guide	Run this command to perform an HTTP upgrade through the management port. If you run the **no http update set oob** command, an HTTP upgrade is performed through a common port. This command can be run on only the devices that support the management port.

❖ Detecting Upgrade Files on the HTTP Server

Command	http check-version

Parameter Description	N/A
Configuration mode	Privileged mode
Usage Guide	Run this command to detect types of upgrade files. The latest upgrade files are detected.

❖ Manually Upgrading Files

Command	http update **{** all **|** ***string*** **}**
Parameter Description	**all**: Upgrades all service modules. *string*: Name of the service module to be upgraded.
Configuration mode	Privileged mode
Usage Guide	Run this command to manually to upgrade the specified service module or all service modules.

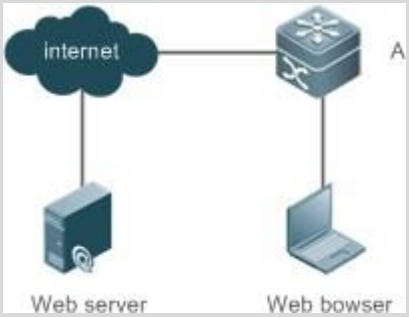
Configuration Example

❖ Using the HTTP Remote Upgrade Function to Upgrade Files

A device obtains upgrade files on QTECH server and downloads the upgrades the files at 02:00 every day.

Check the current upgrade files.

Download the latest files from the server provided by QTECH and update the upgrade device.

Scenario Figure 5-3	
Configuration Steps	▪ Configure the DNS. ▪ Set the scheduled remote monitoring time to 02:00 on the device. ▪ Obtain upgrade files from the remote server. ▪ Download files from the server and update the device.
A	A#configure terminal A(config)# ip domain-lookup A(config)# ip name-server 192.168.58.110 A(config)# http update time daily 02:00 A(config)# http check-version A(config)# end A# http update all
Verification	N/A

Common Errors

When the DNS is disabled, a connection cannot be established between a device and a server.

5.5. Monitoring

Displaying

Description	Command
Displays the configuration and status of the Web service.	**show web-server status**

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
- RFC5424: The_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

Network topology 1 shows the 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.

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
```

6.3.1. The following describes each field in the log in details:

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)

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.

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.

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.

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.

Level

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

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.

Content

This field indicates the detailed content of the syslog.

❖ RFC5424 Log Format

The syslog format in the output direction is as follows:

```
<priority>version timestamp sysname MODULE LEVEL MNEMONIC [structured-data] description
```

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

```
<133>1 2013-07-24T12:19:33.130290Z QTECH SYS 5 CONFIG - Configured from console by console
```

The following describes each field in the log in details:

Priority

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. When the RFC5424 format is enabled, the default value of the facility field is local0 (16).

Version

According to RFC5424, the version is always 1.

Timestamp

The timestamp records the time when a syslog is generated so that you can display and check the system event conveniently. QTECH devices use the following uniformed timestamp format when the RFC5424 logging function is enabled:

```
YYYY-MM-DDTHH:MM:SS.SECFRACZ
```

The following table describes each parameter of the timestamp.

Timestamp Parameter	Description	Remark
YYYY	Year	YYYY indicates the current year.
MM	Month	MM indicates the current month.
DD	Day	DD indicates the current date.
T	Separator	The date must end with "T".
HH	Hour	HH indicates the current hour.
MM	Minute	MM indicates the current minute.
SS	Second	SS indicates the current second.
SECFRAC	Millisecond	SECFRAC indicates the current millisecond (1–6 digits).
Z	End mark	The time must end with "Z".

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.

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.

Level

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

Mnemonic

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

Structured-Data

Structured-data introduced in RFC5424 is parsed as a whole string containing parameter information. Each log may contain 0 or multiple parameters. If a parameter is null, replace this parameter with a placeholder (-). The format of this field is as follows:

```
[SD_ID@enterpriseID PARAM-NAME=PARAM-VALUE]
```

The following table describes each parameter of the structured-data field.

Parameter in structured-data	Description	Remarks
SD_ID	Parameter information name	The parameter information name is capitalized, and must be unique in a log.
@	Separator	"@enterpriseID" is added only to the customized parameter information, not to the parameter information defined in RFC5424.

enterpriseID	Enterprise ID	The enterprise ID is maintained by the Internet Assigned Numbers Authority (IANA). QTECH Networks' enterprise ID is 4881. You can query the enterprise ID on the official website of IANA. http://www.iana.org/assignments/enterprise-numbers
PARAM-NAME	Parameter name	The parameter name is capitalized, and must be unique in the structured-data of a log.
PARAM-VALUE	Parameter value	The parameter value must be enclosed in double quotation marks. Values of the IP address or MAC address must be capitalized, and other types of values are capitalized as required.

description

This field indicates the 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.

6.3.2. 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.

6.3.3. Syslog Format

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

Related Configuration

❖ Enabling the RFC5424 Log Format

By default, the RFC5424 log format is disabled.

After the new format (RFC5424 log format) is enabled, the **service sequence-numbers, service sysname, service timestamps**, **service private-syslog**, and **service standard-syslog** that are applicable only to the old format (RFC3164 log format) lose effect and are hidden.

After log format switchover, the outputs of the **show logging** and **show logging config** commands change accordingly.

❖ 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.

6.3.4. 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**{ *ip-address* | **ipv6** *ipv6-address* } [**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* } [*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 Number of Log Files

By default, the number of log files is 16.

Run the **logging file numbers** *numbers* command in global configuration mode to configure the number of log files.

❖ 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, syslogs 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.

6.3.5. 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.

6.3.6. Featured Logging

The featured logging functions include level-based logging, delayed logging, and periodical logging. If the RFC5424 log format is enabled, logs can be sent in all directions, delayed logging is enabled, and periodical logging is disabled by default. If the RFC5424 log format is disabled, level-based logging, delayed logging, and periodical logging are disabled.

Working Principle

❖ Level-based Logging

You can use the level-based logging function to send syslogs to different destinations based on different module and severity level. For example, you can configure commands to send WLAN module logs of Level 4 or lower to the log server, and WLAN module logs of Level 5 or higher to local log files.

❖ Delayed Logging

After generated, logs are not directly sent to the log server, and instead they are buffered in the log file. The device sends the log file to the syslog server through FTP at a certain interval. This function is called delayed logging.

If the device generates too many logs, sending all logs to the server in real time may deteriorate the performance of the device and the syslog server, and increase the burden of the network. In this case, the delayed logging function can be used to reduce the packet interaction.

By default, the log file sent to the remote server is named ***File size_Device IP address_Index*.txt**. If the prefix of the log file name is modified, the log file sent to the remote server is named ***Configured file name prefix_File size_Device IP address_Index*.txt**. The file stored on the local Flash of the device is named ***Configured file name prefix_Index*.txt**. By default, the file name prefix is syslog_ftp_server, the delayed logging interval is 3600s (one hour), and the log file size is 128 KB.

The maximum value of the delayed logging interval is 65535s, that is, 18 hours. If you set the delayed logging interval to the maximum value, the amount of logs generated in this period may exceed the file size (128 KB). To prevent loss of logs, logs will be written into a new log file, and the index increases by 1. When the timer expires, all log files buffered in this period will be sent to the FTP or TFTP server at a time.

The Flash on the device that is used to buffer the local log files is limited in size. A maximum of eight log files can be buffered on the device. If the number of local log files exceeds eight before the timer expires, all log files that are generated earlier will be sent to the FTP or TFTP server at a time.

- Periodical Logging

Logs about performance statistics are periodically sent. All periodical logging timers are managed by the syslog module. When the timer expires, the syslog module calls the log processing function registered with each module to output the performance statistic logs and send logs in real time to the remote syslog server. The server analyzes these logs to evaluate the device performance.

By default, the periodical logging interval is 15 minutes. To enable the server to collect all performance statistic logs at a time, you need to set the log periodical logging intervals of different statistic objects to a common multiple of them. Currently, the interval can be set to 0, 15, 30, 60, or 120. 0 indicates that periodical logging is disabled.

Related Configuration

- Configuring the Level-based Logging Policy

By default, device logs are sent in all directions.

Run the **logging policy module** *module-name* [**not-lesser-than**] *level* **direction** { **all** | **server** | **file** | **console** | **monitor** | **buffer** } command in global configuration mode to configure the level-based logging policy.

- Enabling Delayed Display of Logs on the Console and Remote Terminal

By default, delayed display of logs on the Console and remote terminal is disabled.

Run the **logging delay-send terminal** command in global configuration mode to enable delayed display of logs on the Console and remote terminal.

❖ Configuring the Name of the File for Delayed Logging

By default, the log file sent to the remote server is named ***File size_Device IP address_Index*.txt**. If the prefix of the log file name is modified, the log file sent to the remote server is named ***Configured file name prefix_File size_Device IP address_Index*.txt**. The file stored on the local Flash of the device is named ***Configured file name prefix_Index*.txt**. The default file name prefix is syslog_ftp_server.

Run the **logging delay-send file flash:***filename* command in global configuration mode to configure the name of the log file that is buffered on the local device.

❖ Configuring the Delayed Logging Interval

By default, the delayed logging interval is 3600s (one hour).

Run the **logging delay-send interval** *seconds* command in global configuration mode to configure the delayed logging interval.

❖ Configuring the Server Address and Delayed Logging Mode

By default, logs are not sent to any FTP or TFTP server.

Run the **logging delay-send server** { [**oob**] *ip-address* | **ipv6** *ipv6-address* } [**vrf** *vrf-name*] **mode** { **ftp user** *username* **password** [**0** | **7**] *password* | **tftp** } command in global configuration mode to configure the server address and delayed logging mode.

❖ Enabling Periodical Logging

By default, periodical logging is disabled.

Run the **logging statistic enable** command in global configuration mode to enable periodical uploading of logs. After this function is enabled, the system outputs a series of performance statistics at a certain interval so that the log server can monitor the system performance.

❖ Enabling Periodical Display of Logs on the Console and Remote Terminal

By default, periodical display of logs on the Console and remote terminal is disabled.

Run the **logging statistic terminal** command in global configuration mode to enable periodical display of logs on the Console and remote terminal.

❖ Configuring the Periodical Logging Interval

By default, the periodical logging interval is 15 minutes.

Run the **logging statistic mnemonic** *mnemonic* **interval** *minutes* command in global configuration mode to configure the periodical logging interval.

6.3.7 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.

	service log-format rfc5424	Enables the RFC5424 syslog format.
Sending Console Syslogs to the	(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	(Optional) It is used to configure parameters for sending syslogs to the monitor terminal.	
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.
	(Optional) It is used to configure parameters for sending syslogs to the log server.	

Sending Syslogs to the Log Server	**logging server** [**oob**] { *ip-address* | **ipv6** *ipv6-address* } [**via** *mgmt-name*] [**udp-port** *port*] [**vrf** *vrf-name*]	Sends logs to a specified log server.
	logging trap [*level*]	Configures the level of logs sent to the log server.
	logging facility *facility-type*	Configures the facility value of logs sent to the log server.
	logging source [**interface**] *interface-type interface-number*	Configures the source interface of logs sent to the log server.
	logging source { **ip** *ip-address* | **ipv6** *ipv6-address* }	Configures the source address of logs sent to the log server.
Writing Syslogs into Log Files	(Optional) It is used to configure parameters for writing syslogs into a file.	
	logging file { **sata0:***filename* | **flash:***filename* | **usb0**:*filename* | **sd0**:*filename* } [*max-file-size*] [level]	Configures parameters for writing syslogs into a file, including the file storage type, file name, file size, and log level.
	logging file numbers *numbers*	Configures the number of files which logs are written into. The default value is 16.
	logging flash interval *seconds*	Configures the interval at which logs are written into log files. The default value is 3600.

	logging life-time level *level days*	Configures the storage time of log files.
Configuring Syslog Filtering	(Optional) It is used to enable the syslog filtering function.	
	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 *module-name* **mnemonic** *mnemonic-name* **level** *level*	Configures the exact-match filtering rule.
	logging filter rule single-match { **level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name* }	Configures the single-match filtering rule.
Configuring Level-based Logging	⚠ (Optional) It is used to configure logging policies to send the syslogs based on module and severity level .	
	logging policy module *module-name* [**not-lesser-than**] *level* **direction** { **all** | **server** | **file** | **console** | **monitor** | **buffer** }	Sends logs to different destinations by module and severity level
	⚠ (Optional) It is used to enable the delayed logging function.	
	logging delay-send terminal	Enables delayed display of lo gs on the

<table>
<tr><td rowspan="4">Configuring Delayed Logging</td><td></td><td>Console and remote terminal.</td></tr>
<tr><td>logging delay-send file flash:filename</td><td>Configures the name of the file on the local
device where logs are buffered.</td></tr>
<tr><td>logging delay-send interval seconds</td><td>Configures the interval at which logs are sent
to the log server.</td></tr>
<tr><td>logging delay-send server { [oob] ip-address | ipv6 ipv6-address } [vrf vrf-name] mode { ftp user username password [0 | 7] password | tftp }</td><td>Configures the server address and delayed logging mode.</td></tr>
<tr><td rowspan="4">Configuring Periodical Logging</td><td colspan="2">⚠ (Optional) It is used to enable the periodical logging function.</td></tr>
<tr><td>logging statistic enable</td><td>Enables the periodical logging function .</td></tr>
<tr><td>logging statistic terminal</td><td>Enables periodical display of logs on the
Console and remote terminal.</td></tr>
<tr><td>logging statistic mnemonic mnemonic interval minutes</td><td>Configures the interval at which logs of a
performance statistic object are sent to the server .</td></tr>
<tr><td rowspan="3">Configuring Syslog Redirection</td><td colspan="2">(Optional) It is used to enable the log redirection function.</td></tr>
<tr><td>logging rd on</td><td>Enables the log redirection function.</td></tr>
<tr><td>logging rd rate-limit number [except severity]</td><td>Configures the log redirection rate limit.</td></tr>
</table>

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

- RFC5424 Log Format

After the RFC5424 log format is enabled, the timestamp is uniform.

In the RFC5424 log format, the timestamp may or may not contain the time zone. Currently, only the timestamp without the time zone is supported.

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.

❖ Enabling the RFC5424 Log Format

(Optional) By default, the RFC5424 log format is disabled.

Unless otherwise specified, perform this configuration on the device to enable the RFC5424 log format.

Verification

Generate a syslog, and check the log format.

Related Commands

❖ Configuring the Timestamp Format of Syslogs

Command	service timestamps **[** ***message-type*** **[** uptime **|** datetime **[** msec **] [** year **]]]**
Parameter Description	*message-type*: 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	By default, logs are displayed in the following format (default format): *timestamp: %module-level-mnemonic: content If the standard syslog format is enabled, logs are displayed in the following format: timestamp %module-level-mnemonic: content 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.

❖ Enabling the Private Syslog Format

Command	service private-syslog
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	By default, logs are displayed in the following format (default format): *timestamp: %module-level-mnemonic: content
	If the private syslog format is enabled, logs are displayed in the following format:
	timestamp module-level-mnemonic: content
	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.

❖ Enabling the RFC5424 Syslog Format

Command	service log-format rfc5424
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	After the new format (RFC5424 log format) is enabled, the **service sequence-numbers**, **service sysname**, **service timestamps**, **service private-syslog**, and **service standard-syslog** commands that are applicable only to the old format (RFC3164 log format) loss effect and are hidden. After log format switchover, the outputs of the **show logging** and **show logging config** commands change accordingly.

Configuration Example

❖ Enabling the RFC3164 Log Format

Scenario	**It is required to configure the timestamp format as follows:** 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	▪ Configure the syslog format.
	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
Verification	After the timestamp format is configured, verify that new syslogs are displayed in the RFC3164 format. ▪ 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.
	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

❖ Enabling the RFC5424 Log Format

Scenario	**It is required to enable the RFC5424 format.**
Configuration Steps	Configure the syslog format.
	QTECH# configure terminal QTECH(config)# service log-format rfc5424
Verification	Verify that new syslogs are displayed in the RFC5424 format. ● 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 new log.
	QTECH(config)#exit <133>1 2013-07-24T12:19:33.130290Z QTECH SYS 5 CONFIG - Configured from console by console QTECH#show logging config Syslog logging: enabled Console logging: level debugging, 4740 messages logged Monitor logging: level debugging, 0 messages logged Buffer logging: level debugging, 4745 messages logged Statistic log messages: disable Statistic log messages to terminal: disable Delay-send file name:syslog_ftp_server, Current write index:3, Current send index:3, Cycle:10 seconds Count log messages: enable Trap logging: level informational, 2641 message lines logged,4155 fail logging to 192.168.23.89

	logging to 2000::1

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
Configuration 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 **[*level*]**
Parameter Description	*level*: Indicates the log level.
Command Mode	Global configuration mode
Configuration 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 **{ *number* |** all ***number* |** console **{*number* |** all ***number* } } [** except **[*severity*]]**
Parameter Description	*number*: 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
Configuration 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.**
Configuration Steps	Configure parameters for displaying syslogs on the Console.
	QTECH# configure terminal QTECH(config)# logging count QTECH(config)# logging console informational QTECH(config)# logging rate-limit console 50
Verification	▪ Run the **show logging config** command to display the configuration.
	QTECH(config)#s how 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

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	*level*: 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:** 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	▪ Configure parameters for displaying syslogs on the monitor terminal.
	QTECH# configure terminal QTECH(config)# logging monitor informational QTECH(config)# line vty 0 4 QTECH(config-line)# monitor
Verification	▪ Run the **show logging config** command to display the configuration.
	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

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 **[*buffer-size*] [*level*]**
Parameter Description	*buffer-size*: Indicates the size of the memory buffer. *level*: 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 syslogs 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	Configure parameters for writing syslogs into the memory buffer.
	QTECH# configure terminal QTECH(config)# logging buffered 131072 informational
Verification	Run the **show logging config** command to display the configuration and recent syslogs.

	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
Configuration Steps	Configure parameters for writing syslogs into the memory buffer.
	QTECH# configure terminal QTECH(config)# logging buffered 131072 informational
Verification	Run the **show logging config** command to display the configuration and recent syslogs.

	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 **] { *ip-address* |** ipv6 ***ipv6-address*** **} [** udp-port ***port*** **] [** vrf ***vrf-name*** **]** **Or** logging **{ *ip-address* |** ipv6 ***ipv6-address*** **} [** udp-prot ***port*** **] [** vrf ***vrf-name*** **]**
Parameter Description	**oob**: Indicates that logs are sent to the log server through the MGMT interface. *ip-address*: Specifies the IP address of the host that receives logs. **ipv6** *ipv6-address*: Specifies the IPv6 address of the host that receives logs. **vrf** *vrf-name*: Specifies the VPN routing and forwarding (VRF) instance connected to the log server. **udp-port** *port*: 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 configure up to five log servers on a QTECH product.

↘ **Configuring the Level of Logs Sent to the Log Server**

Command	logging trap [*level*]
Parameter Description	*level*: 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 ***facility-type***
Parameter Description	*facility-type*: 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 **]** ***interface-type interface-number***
Parameter Description	*interface-type*: Indicates the interface type. *interface-number*: 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	☐ Configure parameters for sending syslogs to the log server.
	QTECH# configure terminal QTECH(config)# logging server 10.1.1.100 QTECH(config)# logging trap debugging QTECH(config)# logging source interface Loopback 0

Verification	Run the **show logging config** command to display the configuration.
	QTECH#s how 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

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

Sylsogs 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 Number of Log Files

(Optional) By default, syslogs are written to 16 log files.

Unless otherwise specified, perform this configuration on the device to configure the number of files which logs are written into.

❖ 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* } [*max-file-size*] [*level*]**

Parameter Description	**flash**: Indicates that log files will be stored on the extended Flash. **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. *filename*: Indicates the log file name, which does not contain a file name extension. The file name extension is always txt.
	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. *level*: Indicates the level of logs that can be written into a log file.
Command Mode	Global configuration mode
Configuration Usage	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. 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. After this command is configured, logs will be written into log files every hour. If you run the **logging flie flash:syslog** command, a total of 16 log files will be created, namely, **syslog.txt**, **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 Number of Log Files

Command	**logging file numbers *numbers***
Parameter Description	*numbers*: Indicates the number of log files. The value ranges from 2 to 32.

Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the number of log files. If the number of log files is modified, the system will not delete the log files that have been generated. Therefore, you need to manually delete the existing log files to save the space of the extended flash. (Before deleting existing log files, you can transfer these log files to an external server through TFTP.) For example, after the function of writing logs into log files is enabled, 16 log files will be created by default. If the device has generated 16 log files and you change the number of log files to 2, new logs will be written into **syslog.txt** and **syslog_1.txt** by turns. The existing log files from **syslog_2.txt** to **syslog_15.txt** will be preserved. You can manually delete these log files.

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

Command	**logging flash interval *seconds***
Parameter Description	*seconds*: 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 *level days***
Parameter Description	*level*: Indicates the log level. *days*: 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. 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.

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	□ Configure parameters for writing syslogs into log files.
	QTECH# configure terminal QTECH(config)# logging file flash:syslog debugging QTECH(config)# logging flash interval 600
Verification	□ Run the **show logging config** command to display the configuration.
	QTECH(config)#show logging config
Configuration Steps	● Configure parameters for writing syslogs into log files.
	QTECH# configure terminal QTECH(config)# logging file flash:syslog debugging QTECH(config)# logging flash interval 600
rification	● Run the **show logging config** command to display the configuration.

```
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
```

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 ***module-name*** mnemonic ***mnemonic-name*** level ***level*** **|** single-match **{** level ***level*** **|** mnemonic ***mnemonic-name*** **|** module ***module-name*** **} }**
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** *module-name*: Indicates the module name. Logs of this module will be filtered out. **mnemonic** *mnemonic-name*: Indicates the mnemonic. Logs with this mnemonic will be filtered out. **level** *level*: Indicates the log level. Logs of this level will be filtered out.
Command Mode	Global configuration mode
Configuration	Log filtering rules include exact-match and single-match.
Usage	The **no logging filter rule exact-match** [**module** *module-name* **mnemonic** *mnemonic-name* **level** *level*]
	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** *level* | **mnemonic** *mnemonic-name* | **module**
	module-name] 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	Configure the syslog filtering function.
	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
Verification	• Run the **show running-config | include loggging** command to display the configuration. • Enter and exit global configuration mode, and verify that the system displays logs accordingly.
	QTECH#configure

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	Configure the syslog filtering function.

	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
Verification	• Run the **show running-config | include loggging** command to display the configuration. • Enter and exit global configuration mode, and verify that the system displays logs accordingly.
	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

6.4.8. Configuring Level-based Logging

Configuration Effect

You can use the level-based logging function to send syslogs to different destinations based on different module and severity level. For example, you can configure a command to send WLAN module logs of Level 4 or lower to the log server, and WLAN module logs of Level 5 or higher to local log files.

Notes

Level-based logging takes effect only when the RFC5424 format is enabled.

Configuration Steps

❖ Configuring Level-based Logging

(Optional) By default, logs are sent in all directions.

Unless otherwise specified, perform this configuration on the device to configure logging polices to send syslogs to different destinations based on module and severity level.

Verification

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

Related Commands

❖ Configuring Level-based Logging

Command	logging policy module ***module-name*** **[** not-lesser-than **]** ***level*** direction **{** all **|** server **|** file **|** console **|** monitor **|** buffer **}**
Parameter Description	*module-name*: Indicates the name of the module to which the logging policy is applied. **not-lesser-than**: If this option is specified, logs of the specified level or higher will be sent to the specified destination, and other logs will be filtered out. If this option is not specified, logs of the specified level or lower will be sent to the specified destination, and other logs will be filtered out. *level*: Indicates the level of logs for which the logging policy is configured. **all**: Indicates that the logging policy is applied to all logs. **server**: Indicates that the logging policy is applied only to logs sent to the log server. **file**: Indicates that the logging policy is applied only to logs written into log files. **console**: Indicates that the logging policy is applied only to logs sent to the Console. **monitor**: Indicates that the logging policy is applied only to logs sent to a remote terminal.

	buffer: Indicates that the logging policy is applied only to logs stored in the buffer.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure logging polices to send syslogs to different destinations based on module and severity level.

Configuration Example

Configuring Level-based Logging

Scenario	**It is required to configure the logging policies as follows:** 1. **Send logs of Level 5 or higher that are generated by the system to the Console.** 2. **Send logs of Level 3 or lower that are generated by the system to the buffer.**
Configuration Steps	Configure the logging policies.
	QTECH# configure terminal QTECH(config)# logging policy module SYS not-lesser-than 5 direction console QTECH(config)# logging policy module SYS 3 direction buffer
Verification	• Run the **show running-config | include logging policy** command to display the configuration. • Exit and enter global configuration mode to generate a log containing module name “SYS”. Verify that the log is sent to the destination as configured.

```
QTECH#show running-config | include logging policy
logging policy module SYS not-lesser-than 5 direction
console logging policy module SYS 3 direction buffer
```

6.4.9. Configuring Delayed Logging

Configuration Effect

By default, delayed logging is enabled by default at the interval of 3600s (one hour). The name of the log file sent to the remote server is ***File size_Device IP address_Index*.txt**. Logs are not sent to the Console or remote terminal.

You can configure the interval based on the frequency that the device generates logs for delayed uploading. This can reduce the burden on the device, syslog server, and network. In addition, you can configure the name of the log file as required.

Notes

This function takes effect only when the RFC5424 format is enabled.

It is recommended to disable the delayed display of logs on the Console and remote terminal. Otherwise, a large amount of logs will be displayed, increasing the burden on the device.

The file name cannot contain any dot (.) because the system automatically adds the index and the file name extension (.txt) to the file name when generating a locally buffered file. The index increases each time a new file is generated. In addition, the file name cannot contain characters prohibited by your file system, such as \, /, :, *, ", <, >, and |. For example, the file name is log_server, the current file index is 5, the file size is 1000 bytes, and the source IP address is 10.2.3.5. The name of the log file sent to the remote server is **log_server_1000_10.2.3.5_5.txt** while the name of the log file stored on the device is **log_server_5.txt**. If the source IP address is an IPv6 address, the colon (:) in the IPv6 address must be replaced by the hyphen (-) because the colon (:) is prohibited by the file system. For example, the file name is log_server, the current file index is 6, the file size is 1000 bytes, and the source IPv6 address is 2001::1. The name of the log file sent to the remote server is **log_server_1000_2001-1_6.txt** while the name of the log file stored on the device is **log_server_6.txt**.

If few logs are generated, you can set the interval to a large value so that many logs can be sent to the remote server at a time.

Configuration Steps

❖ Enabling Delayed Display of Logs on Console and Remote Terminal

(Optional) By default, delayed display of logs on the Console and remote terminal is disabled.

Unless otherwise specified, perform this configuration on the device to enable delayed display of logs on the Console and remote terminal.

❖ Configuring the Name of the File for Delayed Logging

(Optional) By default, the name of the file for delayed logging is ***File size_Device IP address_Index*.txt**.

Unless otherwise specified, perform this configuration on the device to configure the name of the file for delayed logging.

❖ Configuring the Delayed Logging Interval

(Optional) By default, the delayed logging interval is 3600s (one hour).

Unless otherwise specified, perform this configuration on the device to configure the delayed logging interval.

❖ Configuring the Server Address and Delayed Logging Mode

(Optional) By default, log files are not sent to any remote server.

Unless otherwise specified, perform this configuration on the device to configure the server address and delayed logging mode

Verification

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

Related Commands

❖ Enabling Delayed Display of Logs on Console and Remote Terminal

Command	logging delay-send terminal
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	N/A.

❖ Configuring the Name of the File for Delayed Logging

Command	logging delay-send file flash:***filename***
Parameter Description	**flash:***filename*: Indicates the name of the file on the local device where logs are buffered.
Command Mode	Global configuration mode

Configuration Usage	This command is used to configure the name of the file on the local device where logs are buffered. The file name cannot contain any dot (.) because the system automatically adds the index and the file name extension (.txt) to the file name when generating a locally buffered file. The index increases each time a new file is generated. In addition, the file name cannot contain characters prohibited by your file system, such as \, /, :, *, ", <, >, and |.
	For example, the configured file name is log_server, the current file index is 5, the file size is 1000 bytes, and the source IP address is 10.2.3.5. The name of the log file sent to the remote server is **log_server_1000_10.2.3.5_5.txt** while the name of the log file stored on the device is **log_server_5.txt**. If the source IP address is an IPv6 address, the colon (:) in the IPv6 address must be replaced by the hyphen (-) because the colon (:) is prohibited by the file system. For example, the file name is log_server, the current file index is 6, the file size is 1000 bytes, and the source IPv6 address is 2001::1. The name of the log file sent to the remote server is **log_server_1000_2001-1_6.txt** while the name of the log file stored on the device is **log_server_6.txt**.

❖ Configuring the Delayed Logging Interval

Command	logging delay-send interval ***seconds***
Parameter Description	*seconds*: Indicates the delayed logging interval. The unit is second.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the delayed logging interval. The value ranges from 600s to 65,535s.

❖ Configuring the Server Address and Delayed Logging Mode

Command	logging delay-send server **{ [** oob **]** ***ip-address*** **|** ipv6 ***ipv6-address*** **} [** vrf ***vrf-name*** **]** mode **{** ftp user ***username*** password **[** 0 **|** 7 **]** ***password*** **|** tftp **}**
Parameter Description	**oob**: Indicates that logs are sent to the server through the MGMT port of the device, that is, by means of out-band communication. *ip-address*: Indicates the IP address of the server that receives logs. **ipv6** *ipv6-address*: Indicates the IPv6 address of the server that receives logs. **vrf** *vrf-name*: Specifies the VRF instance connected to the log server. *username*: Specifies the user name of the FTP server. *password*: Specifies the password of the FTP server. **0**: (Optional) Indicates that the following password is in plain text. **7**: Indicates that the following password is encrypted.
Command Mode	Global configuration mode
Configuration Usage	This command is used to specify an FTP or a TFTP server for receiving the device logs. You can configure a total of five FTP or TFTP servers, but a server cannot be both an FTP and TFTP server.. Logs will be simultaneously sent to all FTP or TFTP servers.

Configuration Example

❖ Configuring Delayed Logging

Scenario	**It is required to configure the delayed logging function as follows:** 1. **Enable the delayed display of logs on the Console and remote terminal.** 2. **Set the delayed logging interval to 7200s (two hours).** 3. **Set the name of the file for delayed logging to syslog_QTECH.** 4. **Set the IP address of the server to 192.168.23.12, user name to admin, password to admin, and logging mode to FTP.**
Configuration Steps	Configure the delayed logging function.

	QTECH# configure terminal QTECH(config)# logging delay-send terminal QTECH(config)# logging delay-send interval 7200 QTECH(config)# logging delay-send file flash:syslog_QTECH QTECH(config)#loggingdelay-sendserver192.168.23.12modeftpuser adminpassword admin
Verification	• Run the **show running-config | include logging delay-send** command to display the configuration. • Verify that logs are sent to the remote FTP server after the timer expires.
	QTECH#show running-config | include logging delay-send logging delay-send terminal logging delay-send interval 7200 logging delay-send file flash:syslog_QTECH logging delay-send server 192.168.23.12 mode ftp user admin password admin

6.4.10. Configuring Periodical Logging

Configuration Effect

By default, periodical logging is disabled. Periodical logging interval is 15 minutes. Periodical display of logs on the Console and remote terminal are disabled.

You can modify the periodical logging interval. The server will collect all performance statistic logs at the time point that is the least common multiple of the intervals of all statistic objects.

Notes

Periodical logging takes effect only when the RFC5424 format is enabled.

The settings of the periodical logging interval and the function of displaying logs on the Console and remote terminal take effect only when the periodical logging function is enabled.

It is recommended to disable periodical display of logs on the Console and remote terminal. Otherwise, a large amount of performance statistic logs will be displayed, increasing the burden on the device.

To ensure the server can collect all performance statistic logs at the same time point, the timer will be restarted when you modify the periodical logging interval of a statistic object.

Configuration Steps

❖ Enabling Periodical Logging

(Optional) By default, periodical logging is disabled.

Unless otherwise specified, perform this configuration on the device to enable periodical logging.

❖ Enabling Periodical Display of Logs on Console and Remote Terminal

(Optional) By default, periodical display of logs on the Console and remote terminal is disabled.

Unless otherwise specified, perform this configuration on the device to enable periodical display of logs on the Console and remote terminal.

❖ Configuring the Periodical Logging Interval

(Optional) By default, the periodical logging interval is 15 minutes.

Unless otherwise specified, perform this configuration on the device to configure the interval at which logs of statistic objects are sent to the server.

Verification

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

Related Commands

❖ Enabling Periodical Logging

Command	logging statistic enable
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	This command is used to enable periodical logging. After this function is enabled, the system outputs a series of performance statistics at a certain interval so that the log server can monitor the system performance.

Enabling Periodical Display of Logs on Console and Remote Terminal

Command	logging statistic terminal
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration	N/A
Usage	

❖ Configuring the Periodical Logging Interval

Command	logging statistic mnemonic ***mnemonic*** interval ***minutes***
Parameter Description	*mnemonic*: Identifies a performance statistic object. *minutes*: Indicates the periodical logging interval. The unit is minute.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the periodical logging interval for a specified performance statistic object. The interval can be set to 0, 15, 30, 60, or 120 minutes. 0 indicates that periodical logging is disabled.

Configuration Example

❖ Configuring Periodical Logging

Scenario	**It is required to configure the l periodical logging function as follows:** 1. **Enable the periodical logging function.** 2. **Enable periodical display of logs on the Console and remote terminal.** 3. **Set the periodical logging interval of the statistic object TUNNEL_STAT to 30 minutes.**
Configuration Steps	▪ Configure the periodical logging function.

	QTECH# configure terminal QTECH(config)# logging statistic enable QTECH(config)# logging statistic terminal QTECH(config)# logging statistic mnemonic TUNNEL_STAT interval 30
Verification	• Run the **show running-config | include logging statistic** command to display the configuration. • After the periodical logging timer expires, verify that logs of all performance statistic objects are generated at the time point that is the least common multiple of the intervals of all statistic objects.
	QTECH#show running-config | include logging statistic logging statistic enable logging statistic terminal logging statistic mnemonic TUNNEL_STAT interval 30

6.4.11. 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 there are two devices in a VSU. The ID of the active device is 1, and the ID of the secondary device is 2. 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 ***number*** **[** except ***level*** **]**

Parameter Description	**rate-limit** *number*: Indicates the maximum number of logs redirected per second. The value ranges from 1 to 10,000. **except** *level*: 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	▪ Configure the syslog redirection function.
	QTECH# configure terminal QTECH(config)# logging rd on QTECH(config)# logging rd rate-limit 100 except critical
Verification	▪ 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.
	QTECH#show running-config | include logging logging rd rate-limit 100 except critical

6.4.12. 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	▪ Configure the syslog monitoring function.
	QTECH# configure terminal QTECH(confi g)# logging

	userinfo QTECH(config)# logging userinfo command-log
Verification	▪ Run the **show running-config | include logging** command to display the configuration. ▪ Run a command in global configuration mode, and verify that the system generates a log.
	QTECH#configure terminal 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

6.4.13. 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	Configure the synchronization function.
	QTECH# configure terminal QTECH(con fig)# line console 0 QTECH(config-line)# logging synchronous
Verification	Run the **show running-config | begin line** command to display the configuration.

	QTECH#show running-config | begin line line con 0 logging synchronous login local 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. 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

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

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

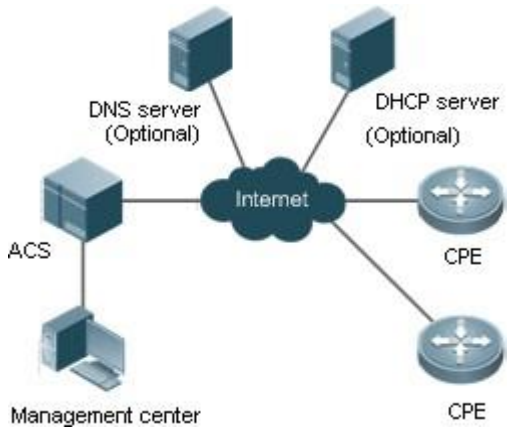
	configuration files, restore the configuration, and realize other features.

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 resolves the names.**

Functional Deployment

HTTP runs on both CPEs and the ACS.

7.3. Features

Basic Concept

❖ Major Terminologies

CPE: Customer Premises Equipment

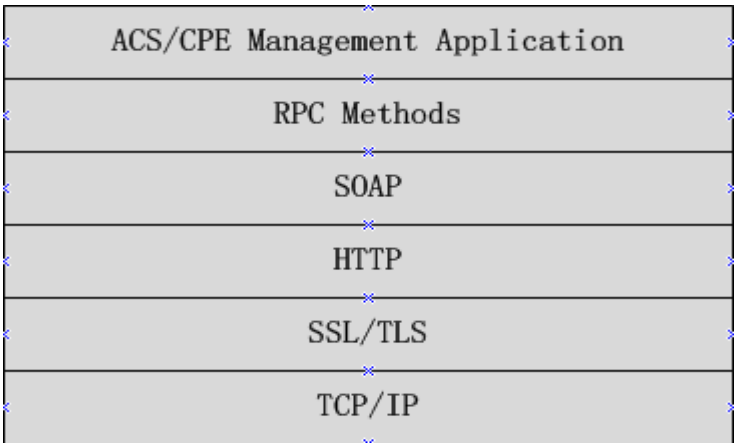
ACS: Auto-Configuration Server

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

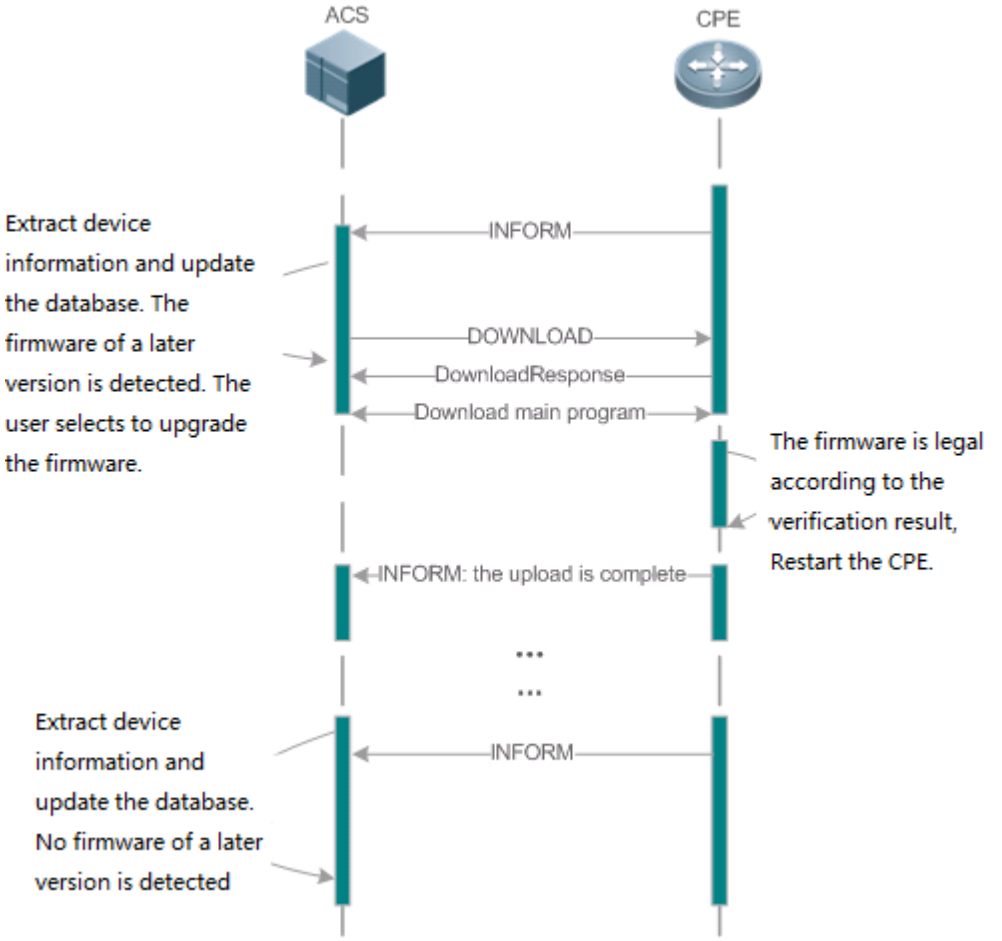
7.3.1. Upgrading the Firmware

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.

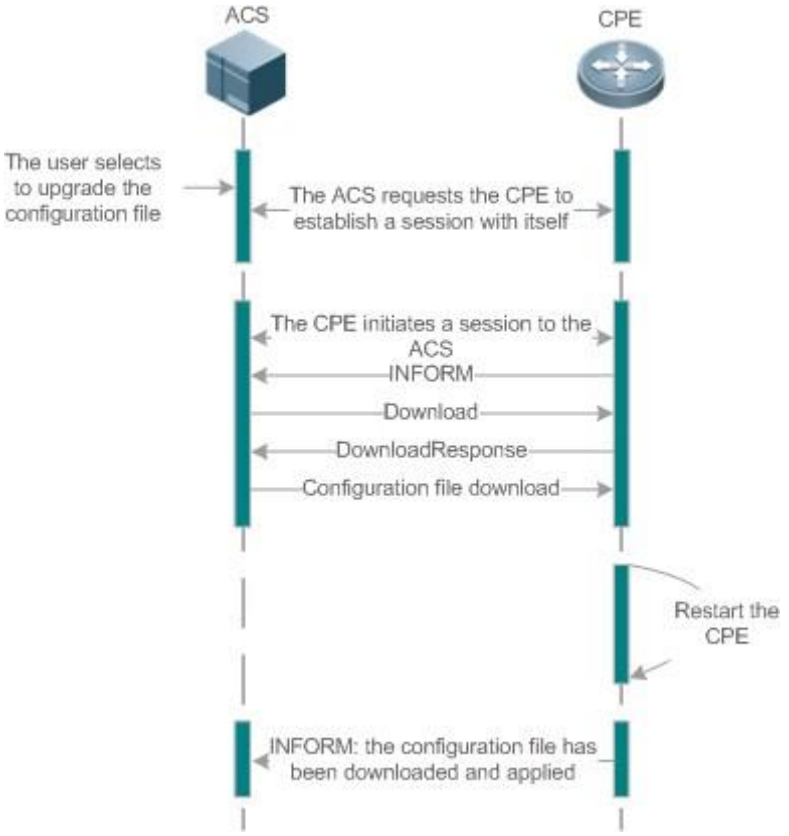
The file server can be ACS or separately deployed.

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.

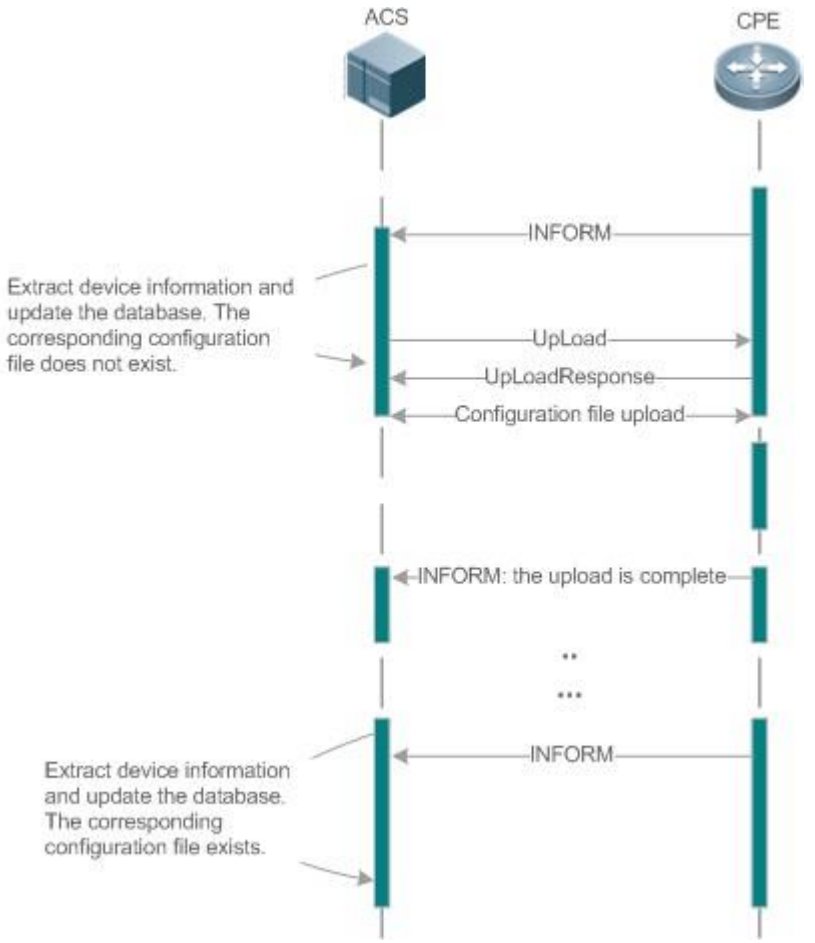
The file server can be ACS or separately deployed.

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. Configuring the Pre-registration Function

The pre-registration function enables a device without configuration to automatically connect to the MACC server and deliver CWMP configurations through the MACC, so that users can go online without perceiving the authentication.

7.3.5. 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.

	（Optional）You can configure the URLs of the CPE and the ACS.	
	acs url	Configures the ACS URL.
	cpe url	Configures the CPE URL.
	cpe source interface	
Configuring CWMP-Related Attributes	(Optional) You can configure the basic functions of the CPE, such as upload, backup and restoration of firmware, configuration files or logs.	
	cpe inform	Configures the periodic notification function of the CPE.

Action	Suggestions and Related Commands	
	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.
	register device	Enables or disables the pre-registeration function.

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 ***username***
Parameter Description	**username** *username*: 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 **{*password* | *encryption-type encrypted-password*}**
Parameter Description	*password:* ACS password *encryption-type:* 0 (no encryption) or 7 (simple encryption) *encrypted-password:* Password text
Defaults	*encryption-type*: 0 *encrypted-password*: 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 ***username***
Parameter Description	*username*: 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 **{*password* | *encryption-type encrypted-password*}**
Parameter	*password:* CPE password *encryption-type:* 0 (no encryption) or 7 (simple encryption)

Description	*encrypted-password:* Password text
Defaults	*encryption-type*: 0
	encrypted-password: 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: • 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 **{** ***url*** **|** macc **}**
Parameter Description	*url*: ACS URL
Defaults	No ACS URL is configured by default.
Command Mode	CWMP configuration mode

Usage Guide	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: ▪ Be in format of **http://host[:port]/path** or **https://host[:port]/path**. ▪ Contain 256 characters at most. Use this command to connect to MACC quickly, achieving the same effect of running the following two commands: ▪ acs url https://cloud.QTECH.com.cn/service/acs cpe inform interval 30

❖ 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	If CPE URL is not configured, it is obtained through DHCP. The CPE URL must: ▪ Be in format of **http://ip [: port]/**. ▪ Contain 256 characters at most.

❖ Configuring the CPE URL for CWMP Connection

Command	cpe source interface ***interface*** **[** port ***port*** **]**
Parameter Description	*interface*: Interface name *port*: Port number
Defaults	N/A

Command Mode	CWMP configuration mode
Usage Guide	This command is incompatible with the **cpe url** command. If both commands are not configured, the CPE will select CPE URL according to the ACS URL. The interface name will be filled in automatically when the CLI command is entered. The default interface number is 7547.

❖ 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	The following example displays the CWMP configuration. QTECH(config-cwmp)#show cwmp configuration
	CWMP Status : enable
	ACS URL : http://www.QTECH.com.cn/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

Configuration Examples

The following configuration examples describe CWMP-related configuration only.

❖ Configuring Usernames and Passwords on the CPE

Network Environment **Figure 7-6**	
Configuration Method	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.
CPE	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
Verification	▪ Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	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/ CPE username : USERB

```
CPE password : ******
```

❖ Configuring the URLs of the ACS and the CPE

Network Environment	**See Figure 7-6.**
Configuration Method	● Configure the ACS URL. ● Configure the CPE URL.

CPE	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/
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	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/

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 126 characters.

The user-input plaintext password contains illegal characters.

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*** **]** **[** start-time ***time*** **]**
Parameter Description	*seconds*: Specifies the periodical notification interval of the CPE. The value range is from 30 to 3,600 in seconds. *time*: 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. ● 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. 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	*seconds*: 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	*seconds*: 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

❖ Configuring Pre-Registration

Pre-registration is enabled by default.

Command register device

Parameter Description

N/A

Defaults

Command Mode

Global configuration mode

Usage Guide

You can run the no register device command to disable pre-registration.

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	The following example displays the CWMP configuration. QTECH(config-cwmp)#show cwmp configuration
	CWMP Status : enable
	ACS URL : http://www.QTECH.com.cn/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

Configuration Examples

❖ Configuring the Periodical Notification Interval of the CPE

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

Configuration Steps	▪ **Enable the CWMP function and enter CWMP configuration mode.** ▪ **Set the periodical notification interval of the CPE to 60 seconds.**
CPE	QTECH#config Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)#cwmp QTECH(config-cwmp)#cpe inform interval 60
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	QTECH #show cwmp configuration CWMP Status : enable …… CPE inform interval : 60s

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

Network Environment	**See Figure 7-6.**
Steps	• Enable the CWMP function and enter CWMP configuration mode. • Disable the function of downloading firmware and configuration files from the ACS.

CPE	QTECH#config Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)#cwmp QTECH(config-cwmp)#disable download
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	QTECH #show cwmp configuration CWMP Status : enable …… CPE download status : disable

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

Network Environment	**See Figure 7-6.**
Configuration Steps	• Enable the CWMP function and enter CWMP configuration mode. • Disable the CPE's function of uploading configuration and log files to the ACS.
CPE	QTECH#config Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)#cwmp QTECH(config-cwmp)# disable upload
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.

CPE	QTECH #show cwmp configuration CWMP Status : enable …… CPE upload status : disable

❖ Configuring the Backup and Restoration Delay

Network Environment	**See Figure 7-6.**
Configuration Steps	• Enable the CWMP function and enter CWMP configuration mode. • Set the backup and restoration delay to 100 seconds.
CPE	QTECH#config Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)#cwmp QTECH(config-cwmp)# cpe back-up Seconds 30
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	QTECH #show cwmp configuration CWMP Status : enable …… CPE back up delay time : 30s

❖ Configuring the ACS Response Timeout of the CPE

Network Environment	**See Figure 7-6.**
Configuration Steps	▪ Enable the CWMP function and enter CWMP configuration mode. ▪ Set the response timeout of the CPE to 100 seconds.

CPE	**QTECH# configure terminal** **Enter configuration commands, one per line.** **End with CNTL/Z. QTECH(config)# cwmp** **QTECH(config-cwmp)# timer cpe-timeout 100**
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	QTECH#show cwmp configuration CWMP Status : enable …… CPE wait timeout : 100s

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.

8.1. 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.

8.2. Applications

Application	Description
Clearing Modulethe Configuration of a	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.

8.2.1. 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:

- Remove the module from the target slot.
- Run the **remove configuration module** command on the device to remove the module configuration.
- Insert a new module into the slot.

8.2.2. 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:

- Run the **remove configuration device** command on the target device.
- Save the configuration.
- Restart the VSU and check whether the configuration of the device is cleared.

8.2.3. 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:

- Run the **no sysmac** command on the target device to delete its MAC address.
- Save the configuration.

- Restart the VSU and check whether the MAC address of the device is reelected.

8.3. Features

Feature

Feature	Description
Automatically Installing the Inserted Module	After a new module is inserted into a chassis-based device, the device's management software will automatically install the module driver.

8.3.1. 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.

8.4. Configuration

The module Hot Swapping feature is automatically implemented without manual configuration.

Configuration	Description and Command	
Clearing Module and Device Configuration	(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 [*device-id* /] *slot-num*	Clears the configuration of a module.
	remove configuration device *device-id*	Clears the configuration of a VSU member device.
	no sysmac	Deletes a MAC configuration address From the file.

8.4.1. 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 **[*device-id/]slot-num***
Parameter Description	*device-id:* 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). *slot-num:* 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 ***device-id***
Parameter Description	*device-id:* 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.

Verification

Run the **show version slot** command to display the installation information of a line card.

Command	show version slots **[*device-id / slot-num*]**
Parameter Description	*device-id*: (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). *slot-num*: (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 24 M8606-24SFP/12GT M8606-24SFP/12GT none 1 3 2 M8606-2XFP M8606-2XFP cannot startup 1 4 24 M8606-24GT/12SFP M8606-24GT/12SFP ok 1 M1 0 N/A M8606-CM master 1 M2 0 N/A none none

Configuration Example

❖ Clearing the Configuration of an Offline Module

Scenario	**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	Run the **remove configuration module** command to delete the card configuration.
	QTECH(config)# remove configuration module 1
	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 24 M8606-24SFP/12GT M8606-24SFP/12GT none 1 3 2 M8606-2XFP M8606-2XFP cannot startup 1 4 24 M8606-24GT/12SFP M8606-24GT/12SFP ok 1 M1 0 N/A M8606-CM master 1 M2 0 N/A none none

8.5. Monitoring

Displaying

Description	Command
Displays the details of a module.	**show version module detail** [*slot-num*] **show version module detail** [device-id/*slot-num*] (in VSU mode)
Displays the online state of a module.	**show version slots** [*slot-num*]

	show version slots [*device-id/slot-num*] (in VSU mode)
Displays the current MAC address of a device.	**show sysmac**
Displays system-level alarm information.	**show alarm**

9.1. 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.

9.2. Applications

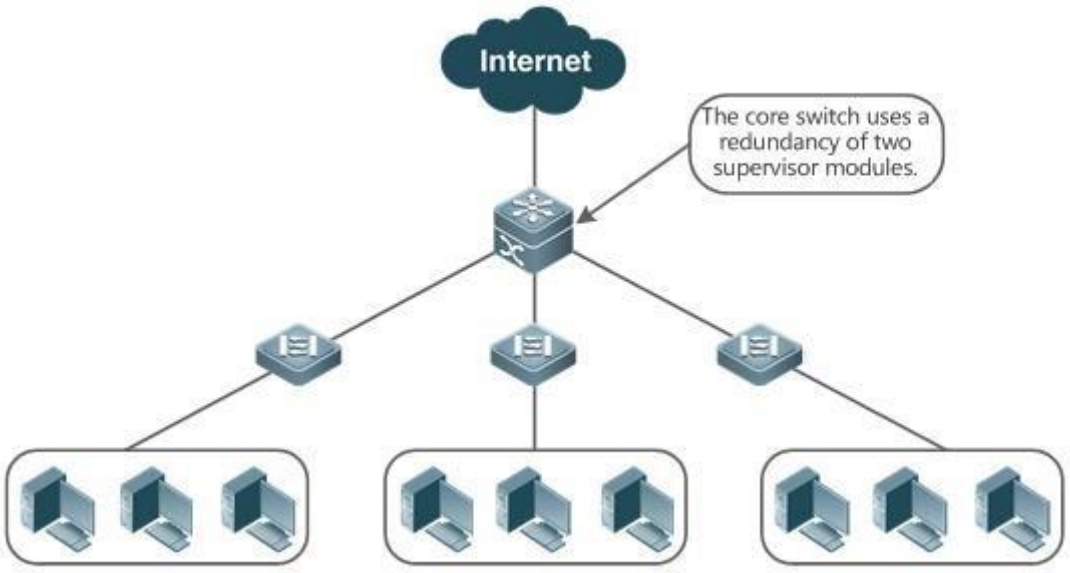
Application	Description
Redundancy of Supervisor Modules	On a core switch where two supervisor modules are installed, the redundancy technology can improve the network stability and system availability.

9.2.1. 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 9-1



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.

9.3. 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
Election of Master and Slave Supervisor Modules	The device can automatically select the master and slave supervisor modules based on the current status of the system. Manual selection is also supported.
Information Synchronization of Supervisor Modules	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.

9.3.1. 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.

9.3.2. 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:

1. The running-config file is synchronized when the device switches from the global configuration mode to privileged EXEC mode.
2. The startup-config file is synchronized when the **write** or **copy** command is executed to save the configuration.
3. 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.

9.4. 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	Optional.	
	redundancy	Enters the redundancy configuration mode.

Automatic Synchronization Interval	**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.

9.4.1. 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.**

	QTECH> enable QTECH# show redundancy states Redundancy role: master Redundancy state: realtime Auto-sync time-period: 3600 s Redundancy management role: master Redundancy control role: active
	Redundancy control 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
Verification	On the original slave supervisor module, run the **show redundancy states** command to check the redundancy status.

	QTECH# show redundancy states Redundancy role: master Redundancy state: realtime Auto-sync time-period: 3600 s Redundancy management role: master Redundancy control role: active Redundancy control state: realtime Auto-sync time-period: 3600 s VSD staff redundancy state: realtime

9.4.2. 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 ***value***

Parameter Description	**time-period *value***: 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.**
	QTECH(config)# redundancy QTECH(config-red)# auto-sync time-period 60 Redundancy auto-sync time-period: enabled (60 seconds). QTECH(config-red)# exit
Verification	Run the **show redundancy states** command to check the configuration.
	QTECH# show redundancy states Redundancy role: master Redundancy state: realtime Auto-sync time-period: 60 s Redundancy management role: master Redundancy control role: active Redundancy control state: realtime Auto-sync time-period: 60 s

9.4.3. 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.**
	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!

Verification	Check whether the relevant supervisor module or device is restarted.

9.5. Monitoring

Displaying

Description	Command
Displays the current redundancy status of dual supervisor modules.	**show redundancy states**

10.1. Overview

The unified forwarding table (UFT) enables the switch to dynamically allocate the hardware forwarding entries.

Protocols and Standards

N/A

10.2. Applications

Typical Application	Scenario
Dynamic Entry Allocation	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.

1.10.2. Dynamic Entry Allocation

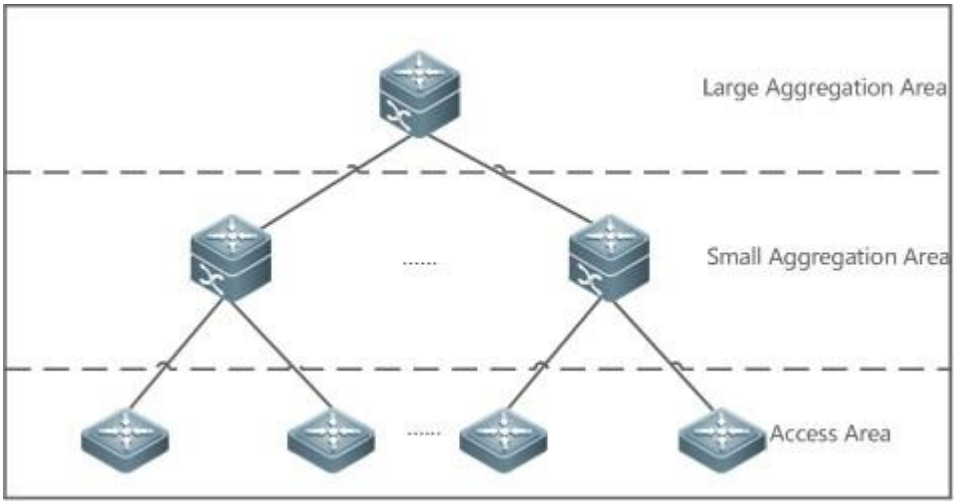
Scenario

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 10-1



Deployment

Enable the switch to operate in Bridge mode of UFT to increase the MAC address table capacity.

- Enable the switch to operate in Default mode of UFT to increase the ARP and ND entry capacity.

10.3. Features

Basic Concepts

N/A

Overview

Feature	Function
UFT operating mode	The UFT provides a mechanism for users to select an operating mode to meet the application scenario needs.

1.10.3. UFT Operating Mode

Working Principle

The UFT provides a mechanism for users to select an operating mode to meet the application scenario needs.

Different devices support different 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 IPv4

The Gateway IPv4 mode does not support IPv6.

❖ Route

The Route mode is dual-stack routing mode, which is applied to routing scenarios and supports both IPv4 and IPv6.

❖ Route IPv4

The Route IPv4 mode is applied to the IPv4 routing scenarios.

❖ 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.

❖ ACL

The ACL mode is applied to ACL scenarios.

10.4. Configuration

Configuration Item	Suggestions and Related Commands
Configuring UFT	Optional configuration. Switch over the current UFT operating mode of the switch.

Operating Mode	**switch-mode** *mode_type* [**overlay**] **slot** *slot_num*	Switches the UFT operating mode in stand-alone mode.

1.10.4. 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 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.

Change the UFT mode and save the change. When the device is restarted for the first time after being upgraded, 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 ***mode_type*** **[** overlay **]** slot ***slot_num***
Parameter Description	*mode_type*: UFT operating mode. *slot_num*: indicates the corresponding line card installed in the chassis.
Defaults	Default mode
Command Mode	Global configuration mode

Usage Guide	▪ In stand-alone mode, the line card can operate in the following modes: ▪ **default**: Default mode, which is applied to most of application scenarios. ▪ **gateway-ipv4**: Gateway IPv4 mode, which is applied to the IPv4 routing scenarios. ▪ **route**: Dual-stack routing mode, which is applied to layer-3 core switches and supports both IPv4 and IPv6. ▪ **route-ipv4**: IPv4 routing mode, which is applied to the IPv4 routing scenarios. ▪ **bridge**: Bridge mode, which is applied to the application scenarios where pure Layer 2 services dominate. ▪ **label**: Label mode, which is applied to the MPLS scenarios. ▪ **acl**: ACL mode, which is applied to the ACL and other security scenarios.

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	QTECH#show switch-mode status Slot No Switch-Mode-Next Switch-Mode-Current 0 bridge bridge0 bridge bridge

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.
	`QTECH(config)#switch-mode bridge slot 3` `Please save current config and restart your device! QTECH(config)#show running-config | include switch-mode switch-mode bridge slot 3`
Check Method	Use the **show switch-mode status** command to display configuration information and UFT mode.
	`QTECH(config)#show switch-mode status Slot No Switch-Mode Status` `3 bridge ok`

Common Errors

-

10.5. Monitoring

Displaying t

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.

11.1. Overview

Package management (pkg_mgmt) is a package management module. This module is responsible for installing, querying and maintaining various components of the device. Through upgrade, users can install new version of software that is more stable or powerful.

Adopting a modular structure, the RGOS system supports overall upgrade and subsystem upgrade.

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 12.0 and later, excluding those upgraded from earlier versions.

Protocols and Standards

N/A

11.2. Applications

Application	Scenario
Upgrading/Degrading Subsystem	Upgrade subsystem like uboot, rboot and main program.
Auto-Sync for Upgrade	Configure the auto sync policy, range and path.

11.2.1. 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. Generally, the subsystem firmware of the box-type device is called main 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 can store the main package in the root directory of the TFTP server, download the package to the device, and then run an upgrade command to upgrade the package locally. You can also store the main

package in a USB flash drive, connect the USB flash drive to the device, and then run an upgrade command to upgrade the package.

11.2.2. 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 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.

11.3. Features

Basic Concepts

❖ Subsystem

A subsystem exists on a device in the form of images. The subsystems of the RGOS include:

- uboot: After being powered on, the device loads and runs the uboot subsystem first. This subsystem is responsible for initializing the device, and loading and running system images.
- rboot: It is used to install and upgrade the main program.Main Program: It is the collection of applications in the system.

❖ Main Package and Rack Package

Main package is often used to upgrade/degrade a subsystem of the box-type device. The main package is a combination package of the uboot, rboot and main program. The main package can be used for overall system upgrade/degradation.

⚠ "Firmware" in this document refers to an installation file that contains a subsystem.

Overview

Feature	Description

Upgrading/Degrading and Managing Subsystems	Upgrades/degrades a subsystem.
Auto-Sync for Upgrade	Ensures uniform upgrade upon member change.

11.3.1. Upgrading/Degrading and Managing Subsystems

Subsystem upgrade/degradation aims to upgrade the software by replacing the subsystems of the device with the subsystems 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.

- uboot: 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.
- rboot: This subsystem exists in a norflash device in the form of images. Therefore, upgrading/degrading this subsystem is to write the image into the norflash device.
- Main Program: 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 subsystems that are available currently and then load subsystems as required. Each subsystem component contains redundancy design. During the upgrade/degradation:

- uboot: 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.
- rboot: as the kernel subsystem contains at least one program. More redundancy backups are allowed if there is enough space.
- Main Program: One redundancy backup is allowed if there is enough space.
- During upgrade of the subsystems, 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.

11.3.2. 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.

11.4. Configuration

Configuration	Description and Command
	The basic function of the configuration is installing and upgrading/degrading a subsystems.

Upgrading/Degrading Firmware a	**upgrade** *url* [**force**]	*url* is a local path where the firmware is stored. This command is used to upgrade the firmware stored on the device.
	upgrade download tftp:/ *path* [**vrf** *vrf-name*] [**force**]	*path* 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 download oob_tftp://*path* **mgmt** { *number* }] [**force**] [**via**	*path* 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 downloadftp://*path vrf-name*] [*force*] [vrf	*path* 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 download oob_ftp:/*/path* [**via mgmt** { *number* }] [**force**]	*path* 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.
Auto-Sync for Upgrade	⚠ (Optional) Configures auto-sync policy.	
	upgrade auto-sync compatible | **coordinate**]	Configures the auto-sync

		policy.
	upgrade auto-sync range [**chassis** | **vsu**]	Configures the auto-sync range.
	upgrade auto-sync package *url*	Configures the auto-sync path.

11.4.1. Upgrading/Degrading a Subsystem

Configuration Effect

Available subsystems include the main package, rack package, and various feature packages.

After the upgrade of the main package is complete, all system software on the line card is updated, and the overall software is enhanced.

Generally a main package is released to upgrade a box-type device.

Notes

N/A

Configuration Steps

Description	**force indicates forced upgrade.**
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Upgrading the Main Package for a Single Device

Optional configuration. This configuration is required when all system software on the device needs to be upgraded.

Download the firmware to the local device and run the **upgrade** command.

Generally a main package is pushed to upgrade a box-type device.

Verification

After upgrading a subsystem, you can run the **show upgrade status** command to check whether the upgrade is successful.

Commands

❖ Upgrade

Command	upgrade ***url*** **[** force **]**
Parameter	*url* indicates firmware directory.

Description	force **indicates forced upgrade.**
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Command	upgrade download tftp:/***path*** **[** vrf ***vrf-name*** **] [** force **]** upgrade download oob_tftp:/***path*** **[** via mgmt **{** ***number*** **}] [** force **]**
Parameter Description	**vrf** *vrf-name* indicates downloading the firmware from the specified VRF. **via mgmt** *number*: If the transfer mode is *oob_tftp* and there are multiple MGMT ports, you can select a specific port. **force** indicates forced upgrade.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Command	upgrade download ftp:/***path*** **[** vrf ***vrf-name*** **] [** force **]** upgrade download oob_ftp:/***path*** **[** force **]**
Parameter Description	**vrf** *vrf-name* indicates downloading the firmware from the specified VRF. **force** indicates forced upgrade.

Command Mode	Privileged EXEC mode
Usage Guide	N/A

❖ Displaying the Firmware Stored on the Device

Command	show upgrade file ***url***
Parameter Description	*url* indicates the path of the firmware in the device file system.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

❖ Displaying Upgrade Status

Command	show upgrade status
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

❖ Displaying Upgrade History

Command	show upgrade history
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuration Example

❖ Example of Upgrading a Subsystems on the Box-Type Device

Network Environment	**Before the upgrade, you must copy the firmware to the device. The upgrade module provides the following solutions.** ▪ **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.** ▪ **Run the** upgrade download tftp://*path* **command directly to upgrade the firmware file stored on the tftp server.** ▪ **Run the** upgrade download ftp://*path* **command directly to upgrade the firmware file stored on the ftp server.** ▪ **Copy the firmware to a USB flash drive, insert 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	Run the upgrade command.
	Check upgrade status during the upgrade process.
	After upgrading the subsystem, restart the device.
	QTECH#upgrade download tftp://172.30.31.176/S6120_RGOS12.1(1)B0101-FULL_install.bin
	*Nov 23 13:21:38: %UPGRADE-6-INFO: Start upgrade
	*Nov 23 13:21:39: %UPGRADE-6-INFO: Copy to /tmp/vsd/0/upgrade_rep/
	*Nov 23 13:21:39: %UPGRADE-6-INFO: Please wait for a moment ....
	Press Ctrl+C to quit
	!!
	!!
	!!
	!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

*Nov 23 13:43:39: %UPGRADE-6-INFO: Upgrade disable reload device

*Nov 23 13:43:39: %UPGRADE-6-INFO: Upgrade disable redundancy forceswitch

```
QTECH#*Nov 23 13:43:41: %UPGRADE-6-INFO: (*2/0) Upgrade processing is 30%
*Nov 23 13:43:45: %UPGRADE-6-INFO: (*2/0) Upgrade get package from master device, wait a moment
*Nov 23 13:46:08: %UPGRADE-6-INFO: (*2/0) Upgrade check package md5 value, wait a moment

*Nov 23 13:46:19: %UPGRADE-6-INFO: (*2/0) Upgrade processing is 60%

*Nov 23 13:46:20: %UPGRADE-6-INFO: Upgrade processing is 10%

*Nov 23 13:46:22: %UPGRADE-6-INFO: Upgrade processing is 30%

*Nov 23 13:46:24: %UPGRADE-6-INFO: Upgrade check package md5 value, wait a moment

*Nov 23 13:46:27: %UPGRADE-6-INFO: (*2/0) Upgrade info [OK]

*Nov 23 13:46:27: %UPGRADE-6-INFO: (*2/0) Rootfs version[1.0.0.e34397af->1.0.0.9e1ff3 ad]
*Nov 23 13:46:27: %UPGRADE-6-INFO: (*2/0) Reload system to take effect !

*Nov 23 13:46:36: %UPGRADE-6-INFO: Upgrade processing is 60%

*Nov 23 13:47:54: %UPGRADE-6-INFO: Upgrade info [OK]

*Nov 23 13:47:54: %UPGRADE-6-INFO: Rootfs version[1.0.0.e34397af->1.0.0.9e1ff3ad]

*Nov 23 13:47:54: %UPGRADE-6-INFO: Reload system to take effect !

*Nov 23 13:48:11: %UPGRADE-6-INFO: Upgrade enable redundancy forceswitch

*Nov 23 13:48:11: %UPGRADE-6-INFO: Upgrade enable reload
```

```
device


*Nov 23 13:48:11: %UPGRADE-6-INFO: Upgrade processing is 100%


*Nov 23 13:48:11: %UPGRADE-6-INFO: Upgrade finishQTECH#upgrade
download          tftp://172.30.31.176/S6120_RGOS12.1(1)B0101-
FULL_install.bin
*Nov 23 13:21:38: %UPGRADE-6-INFO: Start upgrade


*Nov     23     13:21:39:     %UPGRADE-6-INFO:     Copy     to
/tmp/vsd/0/upgrade_rep/


*Nov 23 13:21:39: %UPGRADE-6-INFO: Please wait for a moment



Press Ctrl+C to quit


!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
moment


*Nov  23  13:46:08:  %UPGRADE-6-INFO:  (*2/0)  Upgrade  check
package md5 value, wait a moment


*Nov 23 13:46:19: %UPGRADE-6-INFO: (*2/0) Upgrade processing
is 60%


*Nov 23 13:46:20: %UPGRADE-6-INFO: Upgrade processing is 10%


*Nov 23 13:46:22: %UPGRADE-6-INFO: Upgrade processing is 30%


*Nov 23 13:46:24: %UPGRADE-6-INFO: Upgrade check package md5
value, wait a moment


*Nov 23 13:46:27: %UPGRADE-6-INFO: (*2/0) Upgrade info [OK]


*Nov    23    13:46:27:    %UPGRADE-6-INFO:    (*2/0)     Rootfs
version[1.0.0.e34397af->1.0.0.9e1ff3 ad]
*Nov  23  13:46:27:  %UPGRADE-6-INFO:  (*2/0)  Reload  system  to
```

	take effect ! *Nov 23 13:46:36: %UPGRADE-6-INFO: Upgrade processing is 60% *Nov 23 13:47:54: %UPGRADE-6-INFO: Upgrade info [OK] *Nov 23 13:47:54: %UPGRADE-6-INFO: Rootfs version[1.0.0.e34397af->1.0.0.9e1ff3ad] *Nov 23 13:47:54: %UPGRADE-6-INFO: Reload system to take effect ! *Nov 23 13:48:11: %UPGRADE-6-INFO: Upgrade enable redundancy forceswitch *Nov 23 13:48:11: %UPGRADE-6-INFO: Upgrade enable reload device *Nov 23 13:48:11: %UPGRADE-6-INFO: Upgrade processing is 100% *Nov 23 13:48:11: %UPGRADE-6-INFO: Upgrade finish Hardware version 1.0B Boot version : 1.4.2(Master) 1.4.2(Slave) Software version : S6120_RGOS 12.1(PL1) Serial number : 1234942570025 Slot 2/0 : RG-S6120-20XS4VS2QXS Hardware version 1.00 Boot version : 1.4.2(Master) 1.4.2(Slave) Software version : S6120_RGOS 12.1(PL1) Serial number : 1234942570022 QTECH#
	QTECH#*Nov 23 13:43:41: %UPGRADE-6-INFO: (*2/0) Upgrade processing is 30% *Nov 23 13:43:45: %UPGRADE-6-INFO: (*2/0) Upgrade get package from master device, wait a moment *Nov 23 13:46:08: %UPGRADE-6-INFO: (*2/0) Upgrade check

```
package md5 value, wait a moment

*Nov 23 13:46:19: %UPGRADE-6-INFO: (*2/0) Upgrade processing is 60%

*Nov 23 13:46:20: %UPGRADE-6-INFO: Upgrade processing is 10%

*Nov 23 13:46:22: %UPGRADE-6-INFO: Upgrade processing is 30%

*Nov 23 13:46:24: %UPGRADE-6-INFO: Upgrade check package md5 value, wait a moment

*Nov 23 13:46:27: %UPGRADE-6-INFO: (*2/0) Upgrade info [OK]

*Nov 23 13:46:27: %UPGRADE-6-INFO: (*2/0) Rootfs version[1.0.0.e34397af->1.0.0.9e1ff3 ad]
*Nov 23 13:46:27: %UPGRADE-6-INFO: (*2/0) Reload system to take effect !

*Nov 23 13:46:36: %UPGRADE-6-INFO: Upgrade processing is 60%

*Nov 23 13:47:54: %UPGRADE-6-INFO: Upgrade info [OK]

*Nov 23 13:47:54: %UPGRADE-6-INFO: Rootfs version[1.0.0.e34397af->1.0.0.9e1ff3ad]

*Nov 23 13:47:54: %UPGRADE-6-INFO: Reload system to take effect !

*Nov 23 13:48:11: %UPGRADE-6-INFO: Upgrade enable redundancy forceswitch

*Nov 23 13:48:11: %UPGRADE-6-INFO: Upgrade enable reload device

*Nov 23 13:48:11: %UPGRADE-6-INFO: Upgrade processing is 100%

*Nov 23 13:48:11: %UPGRADE-6-INFO: Upgrade finishQTECH#upgrade download tftp://172.30.31.176/S6120_RGOS12.1(1)B0101-FULL_install.bin
*Nov 23 13:21:38: %UPGRADE-6-INFO: Start upgrade

*Nov 23 13:21:39: %UPGRADE-6-INFO: Copy to /tmp/vsd/0/upgrade_rep/
```

	*Nov 23 13:21:39: %UPGRADE-6-INFO: Please wait for a moment Press Ctrl+C to quit !! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! moment *Nov 23 13:46:08: %UPGRADE-6-INFO: (*2/0) Upgrade check package md5 value, wait a moment *Nov 23 13:46:19: %UPGRADE-6-INFO: (*2/0) Upgrade processing is 60% *Nov 23 13:46:20: %UPGRADE-6-INFO: Upgrade processing is 10% *Nov 23 13:46:22: %UPGRADE-6-INFO: Upgrade processing is 30% *Nov 23 13:46:24: %UPGRADE-6-INFO: Upgrade check package md5 value, wait a moment *Nov 23 13:46:27: %UPGRADE-6-INFO: (*2/0) Upgrade info [OK] *Nov 23 13:46:27: %UPGRADE-6-INFO: (*2/0) Rootfs version[1.0.0.e34397af->1.0.0.9e1ff3 ad] *Nov 23 13:46:27: %UPGRADE-6-INFO: (*2/0) Reload system to take effect ! *Nov 23 13:46:36: %UPGRADE-6-INFO: Upgrade processing is 60% *Nov 23 13:47:54: %UPGRADE-6-INFO: Upgrade info [OK] *Nov 23 13:47:54: %UPGRADE-6-INFO: Rootfs version[1.0.0.e34397af->1.0.0.9e1ff3ad] *Nov 23 13:47:54: %UPGRADE-6-INFO: Reload system to take effect !

```
*Nov 23 13:48:11: %UPGRADE-6-INFO: Upgrade enable redundancy
forceswitch

*Nov 23 13:48:11: %UPGRADE-6-INFO: Upgrade enable reload
device

*Nov 23 13:48:11: %UPGRADE-6-INFO: Upgrade processing is 100%

*Nov 23 13:48:11: %UPGRADE-6-INFO: Upgrade finish
    Hardware version    1.0B

    Boot version : 1.4.2(Master) 1.4.2(Slave)

    Software version : S6120_RGOS 12.1(PL1)

    Serial number : 1234942570025

  Slot 2/0 : RG-S6120-20XS4VS2QXS

    Hardware version    1.00

    Boot version : 1.4.2(Master) 1.4.2(Slave)

    Software version : S6120_RGOS 12.1(PL1)
    Serial number : 1234942570022 QTECH#
```

11.4.2. 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.

vsu: 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 EXEX mode
Usage Guide	It is recommended to set **coordinate**.

❖ 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 EXEX mode
Usage Guide	It is recommended to set **VSU** to ensure uniformity

❖ Configuring Auto-Sync Path

command	upgrade auto-sync package ***url***
Parameter Description	*url* indicates the path of the firmware in the device file system.
Command Mode	Privileged EXEX mode
Usage Guide	The path is not set generally.

Configuration Example

❖ Configuring Auto-Sync Policy

Configuration Steps	**Configure the auto-sync policy.**
	QTECH# upgrade auto-sync policy coordinate
Verification	Check the auto-sync policy. QTECH#show upgrade auto-sync auto-sync range : vsu auto-sync policy : coordinate auto-sync package : flash:install_file/S6120_install.bin

❖ Configuring Auto-Sync Range

Configuration Steps	**Configure the auto-sync range.**
	QTECH# upgrade auto-sync range vsu
Verification	Check the auto-sync range. QTECH#show upgrade auto-sync auto-sync policy: coordinate auto-sync range: vsu auto-sync package: flash:/eg1000m_main_1.0.0.0f328e91.bin

Common Errors

url is not valid.

11.5. Monitoring

Displaying

Function	Command
Displays upgrade status.	**show upgrade status**
Displays the upgrade history.	**show upgrade history**

12.1. 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

OpenFlow Switch Specification Version 1.3.0

12.2. Typical Application

Typical Application	Scenario
Centralized Control	Perform centralized management of authentication.

12.2.1. Centralized Control

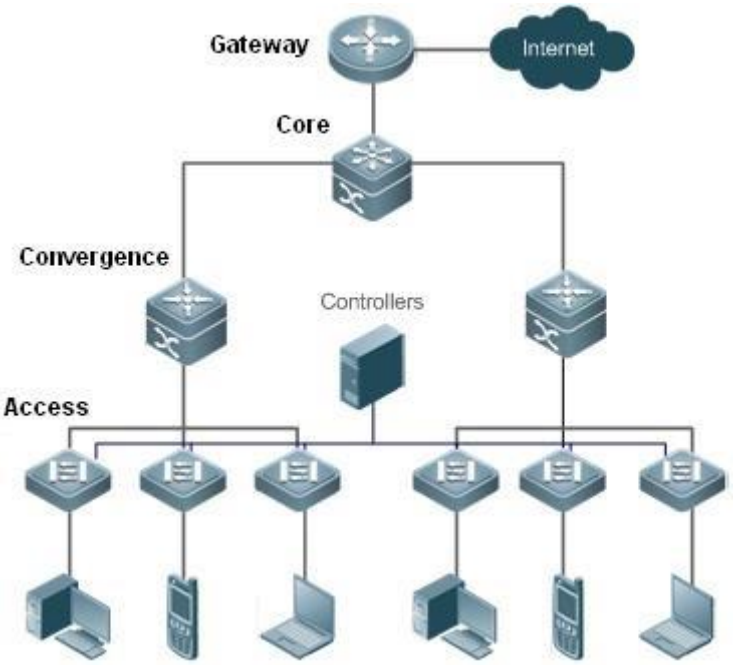
Application Scenario

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 12-1



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.

12.3. 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
Separating Control from Forwarding	Separate the data layer from the control layer of a network device.

12.3.1. Separating Control from Forwarding

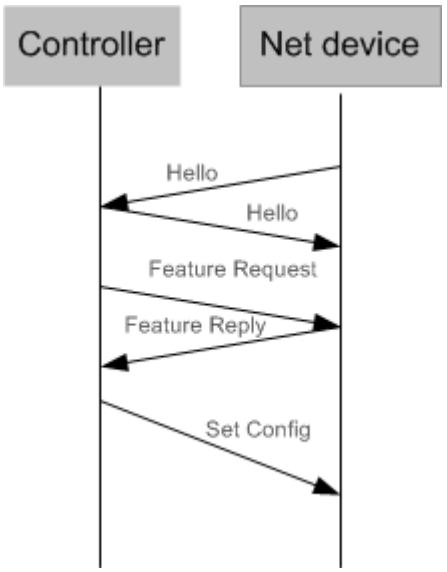
Perform centralized management of the network control plane, so that the entire network is centrally managed at ease (as compared with the status quo of the network), thereby reducing maintenance and management costs.

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. 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.

shows the specific actions involved in this process. Figure 12-2



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 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.

). Then the controller delivers specific user configurations (such as Set Config shown in 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.

) 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.

12.4. Configuration Details

Action	Suggestions and Related Commands	
Configuring OpenFlow	Mandatory configuration, which is used to enable OpenFlow.	
	of controller-ip	Enables the OpenFlow function
	no of controller-ip	Disables the OpenFlow function
Configuring OpenFlow multi-controller	Optional configuration, which is used to configure the multi/single controller mode.	
	of mode [**single** | **multiple**]	Enables the multi/single controller mode
	no of mode	Restores to the single-controller mode.
Configuring VLAN Tag	⚠ Optional configuration, which is used to tag the VLAN packets.	
	of packet vlantag	Tags the VLAN packets sent to the controller.
	no of packet vlantag	Untags the VLAN packets sent to the controller.
ConfiguringTable-Lookup Mode	⚠ Optional configuration, which is used to enable or disable table-lookup.	
	of packet table-lookup [enable| disable]	Enable or disable table-lookup
	no of packet table-lookup	Restores to the default settings.
Configuring Source_IP	⚠ Optional configuration, which is used to configure the source IP address for the OpenFlow controller.	

	of source-ip	Configures the source IP.

12.4.1. 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.

The in-band Ethernet interface connected to the controller is not shown in the output of the **show of port** command.

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	of controller-ip ***ip-address*** **[** port ***port-value*** **] [** aux **]** 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 6653. **aux**: Auxiliary session(available in OpenFlow1.3) **Interface** *interface-id*: port ID, which can be either an out-of-band management interface or a common in-band Ethernet interface.

Command Mode	Global configuration mode
Usage Guide	-

❖ Disabling the OpenFlow Function

Command	no of controller-ip **[*ip-address*]**
Parameter Description	**controller-ip** *ip-address*: Controller IP address
Command Mode	Global configuration mode
Usage Guide	Run this command before switching the controller.

❖ Displaying the Connection Status Between the OpenFlow Device and the Controller

Command	show of
Parameter Description	**-**
Command Mode	Global configuration mode
Usage Guide	-

❖ Displaying Flow Table Entries of the OpenFlow Device

Command	show of flowtable
Parameter Description	**-**
Command Mode	Global configuration mode
Usage Guide	-

❖ Displaying Port Information About the OpenFlow Device

Command	show of port

Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	-

❖ Displaying Group Information about the OpenFlow Device

Command	show of group
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	Only available in OpenFlow1.3

❖ Displaying Meter Information about the OpenFlow Device

Command	show of meter
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	Only available in OpenFlow1.3

Displaying Merged Flow Information about the OpenFlow Device

Command	show of mergedflow
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	Only available in OpenFlow1.3

Disabling LLDP

Command	no lldp enable
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Examples

❖ Configuring the IP Address and Access Port (6633 for OpenFlow1.0 and 6653 for OpenFlow1.3 by Default) of the Controller to Connect the Network Device

Network Environment Figure 12-3	
Configuration Method	Enable the OpenFlow function on the network device and specify the controller IP address.
	QTECH(config)#interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)#no switchport QTECH(config-if-GigabitEthernet 0/1)#ip address 172.18.2.36 255.255.255.0 QTECH(config-if-GigabitEthernet 0/1)#exit QTECH(config)# of controller-ip 172.18.2.35 interface gigabitEthernet 0/1 or QTECH(config)# of controller-ip 172.18.2.35 port 6653 interface gigabitEthernet 0/1
Verification	Display the connection status between the OpenFlow device and the controller, port status and flow table status.

```
OpenFlow1.0 QTECH# show of
Controller is 172.18.2.35 port 6633,connected.



QTECH#show of port
STP is controlled by SDN Controller.

ID                    IFX                    INTERFACE
CONFIG      SPEED     LINK    DUPLEX

2              2                GigabitEthernet   0/2
0x0000      Unknown   DOWN    Unknown

3              3                GigabitEthernet   0/3
0x0000      Unknown   DOWN    Unknown

4              4                GigabitEthernet   0/4
0x0000      Unknown   DOWN    Unknown

5              5                GigabitEthernet   0/5
0x0000      Unknown   DOWN    Unknown

6              6                GigabitEthernet   0/6
0x0000      Unknown   DOWN    Unknown

7              7                GigabitEthernet   0/7
0x0000      Unknown   DOWN    Unknown

8              8                GigabitEthernet   0/8
0x0000      Unknown   DOWN    Unknown

9              9                GigabitEthernet   0/9
0x0000      Unknown   DOWN    Unknown

10            10                GigabitEthernet   0/10
0x0000      Unknown   DOWN    Unknown

11            11                GigabitEthernet   0/11
```

```
0x0000      Unknown   DOWN    Unknown

12            12              GigabitEthernet   0/12
0x0000      Unknown   DOWN    Unknown

13            13              GigabitEthernet   0/13
0x0000      Unknown   DOWN    Unknown

14            14              GigabitEthernet   0/14
0x0000      Unknown   DOWN    Unknown

15            15              GigabitEthernet   0/15
0x0000      Unknown   DOWN    Unknown

16            16              GigabitEthernet   0/16
0x0000      Unknown   DOWN    Unknown


QTECH#show of flowtable

openflow flow count = 1

**************************FLOW
START*****************************

KEY:

          SMAC                DMAC                  SIP
DIP

   00:d0:f8:56:d3:22    00:d0:f8: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

           3ffff2 NA  NA

        PRIORITY       IDLE_TIMEOUT       HARD_TIMEOUT
SEND_FLOW_REM

           120 0 0  0


ACTION:

ACTION_SIZE = 8

OUTPUT_PORT = 7

*****************************FLOW
END*********************************


OpenFlow1.3

QTECH(config)#show of

[0]  Controller  ID=0  Info=tcp:172.18.2.35  port=6653
interface GigabitEthernet 0/1, Main is Connected, Aux
is Disabled


QTECH#show of port

STP is controlled by SDN Controller.
```

```
ID  IFX  INTERFACE  SPEED  LINK  DUPLEX  TX_PKT  RX_PKT
CONFIG

2       2       GigabitEthernet 0/2   Unknown     DOWN
Unknown     0             0             NA

3       3       GigabitEthernet 0/3   Unknown     DOWN
Unknown     0             0             NA

4       4       GigabitEthernet 0/4   Unknown     DOWN
Unknown     0             0             NA

5       5       GigabitEthernet 0/5   Unknown     DOWN
Unknown     0             0             NA

6       6       GigabitEthernet 0/6   Unknown     DOWN
Unknown     0             0             NA

7       7       GigabitEthernet 0/7   Unknown     DOWN
Unknown     0             0             NA

8       8       GigabitEthernet 0/8   Unknown     DOWN
Unknown     0             0             NA

9       9       GigabitEthernet 0/9   Unknown     DOWN
Unknown     0             0             NA

10      10      GigabitEthernet 0/10  Unknown     DOWN
Unknown     0             0             NA

11      11      GigabitEthernet 0/11  Unknown     DOWN
Unknown     0             0             NA

12      12      GigabitEthernet 0/12  Unknown     DOWN
Unknown     0             0             NA

13      13      GigabitEthernet 0/13  Unknown     DOWN
Unknown     0             0             NA
```

```
14      14       GigabitEthernet  0/14  Unknown     DOWN
Unknown     0             0            NA

15      15       GigabitEthernet  0/15  Unknown     DOWN
Unknown     0             0            NA

16      16       GigabitEthernet  0/16  Unknown     DOWN
Unknown     0             0            NA



QTECH#show of flowtable

/************************** openflow flow table[ 0]---flow number:1
**********************/
{table="0", duration_sec="0", priority="500", idle_timeout="0",
hard_timeout="0",        cookie="0x0",        packet_count="0",
byte_count="0".                          match=oxm{in_port="2",
eth_src="00:d0:f8:56:d3:22",                  eth_type="0x800"}
instructions=[apply{acts=[output{port="controller",
max_len="65535"}]}]}



/************************  openflow  flow  table[    1]---flow
number:0 **********************/




/************************  openflow  flow  table[    2]---flow
number:0 **********************/




/************************  openflow  flow  table[    3]---flow
number:0 **********************/




/************************    openflow    flow    table    end
************************************/ flow total number = 1

QTECH(config)#
```

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.

1.12.4. Configuring OpenFlow Multi-controller

Configuration Effect

You can connect multiple controllers once.

Notes

Disable the OpenFlow function, configure the controller mode and then enable the OpenFlow function.

Configuration Method

❖ Disabling OpenFlow

Disable the OpenFlow function first.

❖ Configuring Controller Mode

You can configure single-controller and multi-controller mode.

❖ Displaying Connection Status

Check the connection status

Verification

Display the connection status using the **show of** command.

Related Commands

❖ Configuring Controller Mode

Command	of mode [single | multiple] no of mod
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	You can use the **no** form of this command to restore the device to

	the single-controller mode.

Displaying OpenFlow Connection Status

Command	show of
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Examples

❖ Configuring Single-controller Mode or Multi-controller Mode

Network Environment Figure 12-4	
Configuration	Configure single-controller mode.
Method	QTECH(config)#of mode single
	QTECH(config)#no of mode
	Configure multi-controller mode.
	QTECH(config)#of mode multiple
Verification	Configure multi-controller mode and connect two controllers.
	QTECH(config)#no of controller-ip

```
QTECH(config)#of mode single
QTECH(config)#of   controller-ip   172.18.122.24   interface   gigabitEthernet   0/1
QTECH(config)#of   controller-ip   172.18.122.25   interface   gigabitEthernet   0/1
Controller Mode is Single, can't connected

QTECH(config)#no      of      controller-ip
```

```
QTECH(config)#of mode multiple

QTECH(config)#of controller-ip 172.18.122.24 interface gigabitEthernet 0/1
QTECH(config)#of controller-ip 172.18.122.25 interface gigabitEthernet 0/1
```

12.4.2. Configuring VLAN Tag

Configuration Effect

Configure whether to contain the VLAN tag in the packet sent by the OpenFlow device. VLAN tag is contained in the packet by default.

Notes

The configuration takes effect immediately.

Configuration Method

❖ Configuring the VLAN Tag Contained in the Packet

Command	of packet vlantag
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

❖ Displaying OpenFlow Connection Status

Command	show of
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

Use wireshark to capture packets to see whether the VLAN tag is contained in the packet sent by the OpenFlow device.

Configuration Example

Network Environment Figure 12-5	
Verification	Use wireshark to capture packets to see whether the VLAN tag is contained in the packet sent by the OpenFlow device.

12.4.3. Configuring Table-Lookup Mode

Configuration Effect

Configure whether to perform table-lookup when the device receives the packet. Table-lookup is enabled by default.

Notes

The configuration takes effect immediately.

Configuration Method

❖ Enabling/Disabling Table-Lookup

Command	of packet table-lookup **[** enable **|** disable **]**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

❖ Displaying OpenFlow Connection Status

Command	show of
Parameter Description	N/A
Command Mode	Global configuration mode

Usage Guide	N/A

Verification

Display the connection status using the **show of** command.

Configuration Examples

❖ Enabling/Disabling Table-Lookup Mode

Network Environment Figure 12-6	
Configuration Method	• Configure the table-lookup mode. QTECH(config)#ofpacket table-lookup enable • Disable the table-lookup mode. QTECH(config)#of packet table-lookup disable • Restore the default setting. QTECH(config)#no ofpacket table-lookup
Verification	Use wireshark to capture packets to see whether table-lookup is enabled. **Action** indicates that table-lookup is enabled while **no match** indicates that table-lookup is disabled. QTECH(config)#show of version:openflow1.3, controller[0]:tcp:172.18.105.11 port 6653 interface GigabitEthernet 1/0/7, main is connected, aux is disable, role is master. Current controller mode : multiple. Current packet process mode : Lookup all flow. Datapath id = 897516188948

12.4.4. Configuring Source IP Address

Configuration Effect

The default source IP address is the IP address of the connection port.

Notes

The configuration takes effect immediately.

Configuration Method

❖ Configuring the Source IP Address

Command	of source-ip ***ip-address***
Parameter Description	*ip-address*: Source IP address.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

Display the source IP address using the **show of** command.

Configuration Examples

❖ Configuring the Source IP Address

Network Environment

Figure 12-7

Configure the source IP address.

Configuration Method

```
QTECH(config)#of source-ip 192.168.197.25
```

Restore the default settings.

```
QTECH(config)#no of source-ip
```

Verification

Use wireshark to capture packets to check whether the IP address is the source IP. Run the **show of**

command to check the current mode.

```
QTECH(config)#show of
version:openflow1.3, controller[0]:tcp:172.18.105.11 port 6653 interface GigabitEthernet 1/0/7, main is connected, aux is disable, role is master.
Current controller mode : multiple.
Current packet process mode : No lookup, packet send to controller direct. Datapath id = 897516188948
Source IP = 192.168.197.25
```

12.5. 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
show of group(only available in OpenFlow1.3)	Displays the group table of the current OpenFlow device
show of meter(only available in OpenFlow1.3)	Displays the meter table of the current OpenFlow device
show of mergedflow(only available in OpenFlow1.3)	Displays the merged flow table of the current OpenFlow device

Displaying Debugging Information

-