QTECH
МИР ДОСТУПНЕЕ

System Configuration

www.qtech.ru

➤

Оглавление

1. CONFIGURING CLI

1.1 Overview

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

Protocols and Standards

N/A

1.2 Applications

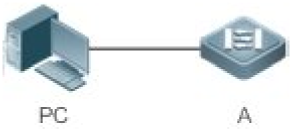
Application	Description
Configuring and Managing Network Devices Through CLI	You can enter commands in the CLI window to configure and manage network devices

1.2.1 Configuring and Managing Network Devices Through CLI

Scenario

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

Figure 1-1



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

Deployment

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.

1.3.1 Accessing CLI

Before using the CLI, you need to connect a terminal or PC to a network device. You can use the CLI after starting the network device and finishing hardware and software initialization. When used for the first time, the network device can be connected only through the console port, which is called out band management. After performing relevant configuration, you can connect and manage the network device through Telnet.

1.3.2 Command Modes

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

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

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

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

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

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

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

1.3.3 System Help

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

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

For example

```
Qtech>?
Exec commands:
  <1 99>      Session number to resume
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  help        Description of the interactive help system
  lock        Lock the terminal
  ping        Send echo messages
  show        Show running system information
  telnet      Open a telnet connection
  traceroute  Trace route to destination
```

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

For example

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

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

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

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

For example

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

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

For example

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

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

For example

```
Qtech(config)#help
```

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

1.3.4 Abbreviated Commands

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

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

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

1.3.5 No and Default Options of Commands

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

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

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

1.3.6 Prompts Indicating Incorrect Commands

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

The following table lists the common CLI error messages.

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

1.3.7 History Commands

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

The methods are described in the following table.

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

The standard terminals, such as the VT100 series, support the direction keys.

1.3.8 Featured Editing

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

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

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

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

```
access list 199 permit ip host 192.168.180.220 host

$ost 192.168.180.220 host 202.101.99.12

$0.220 host 202.101.99.12 time range tr
```

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

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

1.3.9 Searching and Filtering of the Show Command Output

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

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

- The **show** command can be executed in any mode.
- Searched contents are case sensitive.

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

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

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

```
Qtech#show running config | include interface

interface GigabitEthernet 0/0

interface GigabitEthernet 0/1

interface GigabitEthernet 0/2
interface GigabitEthernet 0/3
interface GigabitEthernet 0/4
interface GigabitEthernet 0/5
interface GigabitEthernet 0/6
interface GigabitEthernet 0/7
interface Mgmt 0
```

1.3.10 Command Alias

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

Configuration Effect

6. 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".

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

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

Configuration Steps

❖ Displaying Default Alias

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

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

➢ These default aliases cannot be deleted.

❖ Configuring a Command Alias

Command	**alias** *mode command-alias original-command*
Parameter Description	*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	Global configuration mode

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

<table>
<tr><td><b>Configuration Steps</b></td><td>In global configuration mode, configure the alias "ir" to represent the default route configuration command <b>ip route</b> <i>0.0.0.0 0.0.0.0 192.168.1.1.</i></td></tr>
<tr><td></td><td><pre>
Qtech#configure terminal
Qtech(config)#alias config ir ip route 0.0.0.0 0.0.0.0 192.168.1.1
</pre></td></tr>
<tr><td></td><td></td></tr>
<tr><td><b>Verification</b></td><td>➢ Run the <b>show alias</b> command to check whether the alias is configured successfully.
<pre>
Qtech(config)#show alias
Exec mode alias:
  h   help
  p   ping
  s   show
  u   undebug
  un   undebug
Global configuration mode alias:
  ir   ip route 0.0.0.0 0.0.0.0 192.168.1.1
</pre></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td>➢ Use the configured alias to run the command, and run the <b>show running-config</b> command to check whether the alias is configured successfully.</td></tr>
<tr><td></td><td><pre>
Qtech(config)#ir
Qtech(config)#show running config
</pre></td></tr>
</table>

	`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.

```
Qtech(config if)#ia ?
  A.B.C.D  IP address
  dhcp     IP Address via DHCP
Qtech(config if)#ip address
```

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

2. CONFIGURING BASIC MANAGEMENT

2.1 Overview

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

2.2 Applications

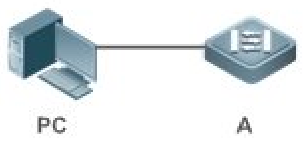
Application	Description
Network Device Management	A user logs in to a network device from a terminal and runs commands on a command line interface (CLI) to manage device configurations.

2.2.1 Network Device Management

Scenario

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

Figure 2-1



2.3 Features

Basic Concepts

❖ TFTP

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

❖ AAA

AAA is short for Authentication, Authorization and Accounting.

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

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

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

AAA provides effective means of network management and security protection.

❖ RADIUS

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

❖ Telnet

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

❖ System Information

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

❖ Hardware Information

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

Overview

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

2.3.1 User Access Control

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

Working Principle

❖ Privilege Level

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

❖ Password Classification

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

❖ Password Protection

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

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

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

❖ Command Authorization

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

Related Configuration

❖ Configuring a Simple Encrypted Password

➢ Run the **enable password** command.

- Configuring a Secure Encrypted Password

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

- Configuring Command Privilege Levels

- Run the **privilege** command to assign a privilege level to a command.
- A command at a lower level is accessible by more users than a command at a higher level.

- Raising/Lowering a User Privilege Level

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

- Enabling Line Password Protection

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

2.3.2 Login Authentication Control

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

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

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

Working Principle

❖ Line Password

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

❖ Local Authentication

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

❖ AAA

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

Related Configuration

❖ Configuring Local User Information

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

❖ Configuring Local Authentication for Line-Based Login

➢ Run the **login local** command (in the case that AAA is disabled).

➢ Perform this configuration on every device.

❖ Configuring AAA Authentication for Line-Based Login

➢ The default authentication method is used after AAA is enabled.

➢ Run the **login authentication** command to configure a login authentication method list for a line.

➢ Perform this configuration when the local AAA authentication is required.

❖ Configuring the Connection Timeout Time

➢ The default connection timeout time is 10 minutes.

➢ Run the **exec-timeout** command to change the default connection timeout time. An established connection will be closed if no output is detected during the timeout time.

➢ Perform this configuration when you need to increase or reduce the connection timeout time.

❖ Configuring the Session Timeout Time

➢ The default session timeout time is 0 minutes, indicating no timeout.

➢ Run the **session-timeout** command to change the default session timeout time.

- ➢ The session established to a remote host through a line will be disconnected if no output is detected during the timeout time. Then the remote host is restored to Idle. Perform this configuration when you need to increase or reduce the session timeout time.

❖ Locking a Session

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

2.3.3 Basic System Parameters

❖ System Time

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

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

❖ Configuring a System Name and Command Prompt

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

❖ Banner

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

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

❖ Configuring the Console Baud Rate

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

❖ Configuring the Connection Timeout Time

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

Related Configuration

- ❖ Configuring the System Date and Clock
- ➢ Run the **clock set** command to configure the system time of a network device manually. The device clock starts from the configured time and keeps running even when the device is powered off.
- ❖ Updating the Hardware Clock
- ➢ If the hardware clock and software clock are not synchronized, run the **clock update-calendar** command to copy the date and time of the software clock to the hardware clock.
- ❖ Configuring a System Name
- ➢ Run the **hostname** command to change the default system name.
- ➢ The default host name is **Qtech**.
- ❖ Configuring a Command Prompt
- ➢ Run the **prompt** command.
- ❖ Configuring Daily Notification
- ➢ By default, no daily notification is configured.
- ➢ Run the **banner motd** command to configure daily notification.
- ➢ Daily notification is displayed on all terminals connected to network devices soon after login. Urgent messages (such as immediate system shutdown) can be delivered to users through daily notification.
- ❖ Configuring a Login Banner
- ➢ By default, no login banner is configured.
- ➢ Run the **banner login** command to configure a login banner to display login information.
- ❖ Configuring the Console Baud Rate
- ➢ Run the **speed** command.
- ➢ The default baud rate is 9,600 bps.

2.3.4 Displaying Configurations

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

Working Principle

- ❖ Running Configurations

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

❖ Startup Configurations

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

Related Configuration

❖ Displaying Running Configurations

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

❖ Displaying Startup Configurations

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

❖ Storing Startup Configurations

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

2.3.5 Telnet

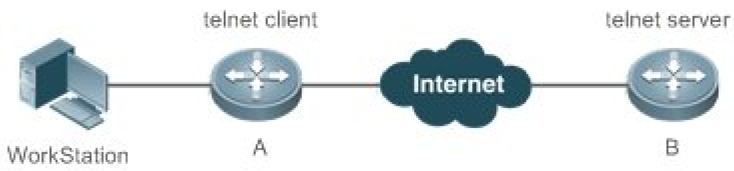
Working Principle

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

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

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

Figure 2-2



Related Configuration

- ❖ Enabling the Telnet Client Service
- ➢ Run the **telnet** command to log in to a remote device.
- ❖ Restoring a Telnet Client Session
- ➢ Run the **<1-99>** command.
- ❖ Disconnecting a Suspended Telnet Client Session
- ➢ Run the **disconnect** *session-id* command.
- ❖ Enabling the Telnet Server Service
- ➢ Run the **enable service telnet-server** command.
- ➢ Perform this configuration when you need to enable Telnet login.

2.3.6 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.
-

2.4 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.
	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 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 a Restart Policy	(Optional) It is used to configure a system restart policy.	
	reload	Restarts a device.

2.4.1 Configuring Passwords and Privileges

Configuration Effect

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

Notes

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

Configuration Steps

❖ Configuring a Simple Encrypted Password

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

❖ Configuring a Secure Encrypted Password

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

❖ Configuring Command Privilege Levels

- Optional.

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

❖ Raising/Lowering a User Privilege Level

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

❖ 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.

❖ 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.

```
Qtech# disable 1
Qtech> reload ?
at                    reload at
```

	`<cr>`

2.4.2 Configuring Login and Authentication

Configuration Effect

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

Configuration Steps

❖ Configuring Local User Information

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

❖ Configuring Local Authentication for Line-Based Login

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

❖ Configuring AAA Authentication for Line-Based Login

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

❖ Enabling the Telnet Client Service

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

❖ Restoring a Telnet Client Connection

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

❖ Closing a Suspended Telnet Client Connection

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

- Enabling the Telnet Server Service

- Optional.
- Enable the Telnet Server service when you need to enable Telnet login.

- Configuring the Connection Timeout Time

- Optional.
- An established connection will be closed if no output is detected during the timeout time.
- Perform this configuration when you need to increase or reduce the connection timeout time.

- Configuring the Session Timeout Time

- Optional.
- The session connecting to a remote host will be disconnected and the host be restored to Idle if no output is detected during the timeout time.
- Perform this configuration when you need to increase or reduce the session timeout time.

- Locking a Session

- (Optional) Perform this configuration when you need to temporarily exit a session on a device.
- To lock a session, first enable terminal lock in line configuration mode, and then run the **lock** command to lock the terminal.

Verification

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

Related Commands

- Configuring Local User Information

Command	**username** *name* [**login mode** { **console** | **ssh** | **telnet** }] [**online amount** *number*] [**permission**

	oper-mode path] [**privilege** *privilege-level*] [**reject remote-login**] [**web-auth**] [**pwd-modify**] [**nopassword** | **password** [**0** | **7**] *text-string*]
Parameter Description	*name*: Indicates a user name. **login mode**: Indicates the login mode. **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.
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.

❖ 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*] [**via** *mgmt-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. **via** *mgmt-name*: Indicates the management port used by the Telnet client when the **oob** option is specified.
Command Mode	Privileged EXEC mode
Usage Guide	A user can telnet to a remote device identified by an IPv4 host name, IPv6 host name, IPv4 address, or IPv6 address.

❖ Restoring a Telnet Client Session

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

❖ Closing a Suspended Telnet Client Connection

Command	**disconnect** *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.

```
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 Steps	➢ Set the session timeout time to 20 minutes.

	`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.

2.4.3 Configuring Basic System Parameters

Configuration Effect

➢ Configure basic system parameters.

Configuration Steps

❖ Configuring the System Date and Clock

➢ Mandatory.

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

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

❖ Updating the Hardware Clock

➢ Optional.

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

❖ Configuring a System Name

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

❖ Configuring a Command Prompt

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

❖ Configuring Daily Notification

➢ (Optional) Perform this configuration when you need to display important prompts or warnings to users.

➢ You can configure notification in one or multiple lines, which will be displayed to users after login.

❖ Configuring a Login Banner

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

❖ Configuring the Console Baud Rate

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

Verification

➢ Run the **show clock** command to display the system time.

➢ Check whether a login banner is displayed after login.

➢ Run the **show version** command to display the system information and version.

Related Commands

❖ Configuring the System Date and Clock

Command	**clock set** *hh:mm:ss month day year*
Parameter Description	*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 Mode	Privileged EXEC mode
Usage Guide	After the configuration, the time of the software clock will overwrite that of the hardware clock.

❖ Configuring a System Name

Command	**hostname** *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	*string*: Indicates the command prompt name. A name with more than 32 characters will be truncated to

Description	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 Verification
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 Verification

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

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
```

2.4.4 Enabling and Disabling a Specific Service

Configuration Effect

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

Configuration Steps

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

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

Verification

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

Related Commands

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

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

Configuration Example

❖ Enabling the SSH Server Service

Configuration Steps	➢ 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.

2.4.5 Configuring a Restart Policy

Configuration Effect

Configure a restart policy to restart a device as scheduled.

Configuration Steps

❖ Configuring Direct Restart

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

❖ Configuring Timed Restart

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

If you configure a specific time, the system will restart at the time. The time must be a time in the future. The **month**, **day** and **year** parameters are optional. If they are not specified, the time of the system clock 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.

2.5 Monitoring

Displaying

Description	Command
show clock	Displays the current system time.
show line { **console** *line-num* | **vty** *line-num* **|** *line-num* }	Displays line configurations.
show reload	Displays system restart settings.
show running-config [**interface** *interface*]	Displays the current running configurations of the device or the configurations on an interface.
show startup-config	Displays the device configurations stored in the NVRAM.
show this	Displays the current system configurations.
show version [**devices | module | slots**]	Displays system information.
show sessions	Displays the information of each established Telnet client instance.

3. CONFIGURING LINES

3.1 Overview

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

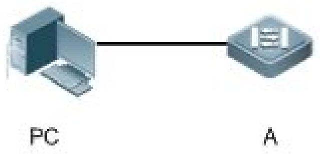
3.2 Applications

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

3.2.1 Accessing a Device Through Console

Scenario

Figure 3-1



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

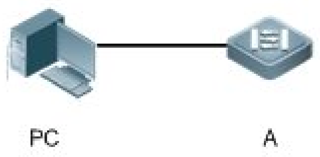
Deployment

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

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

3.4.1 Entering Line Configuration Mode

Configuration Effect

Enter line configuration mode to configure other functions.

Configuration Steps

❖ Entering Line Configuration Mode

➢ Mandatory.

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

❖ Increasing/Reducing the Number of VTY Lines

➢ Optional.

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

Verification

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

Related Commands

❖ Entering Line Configuration Mode

Command	**line** [**aux** | **console** | **tty** | **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

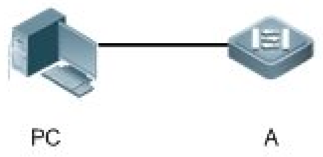
Command	**line vty** *line-number*
Parameter Description	*line-number*: Indicates the number of VTY lines. The value ranges from 0 to 35.
Command Mode	Global configuration mode
Usage Guide	Run the **no line vty** *line-number* command to reduce the number of available VTY lines.

❖ Displaying Line Configuration

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

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* }

4. CONFIGURING TIME RANGE

4.1 Overview

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

4.2 Typical Application

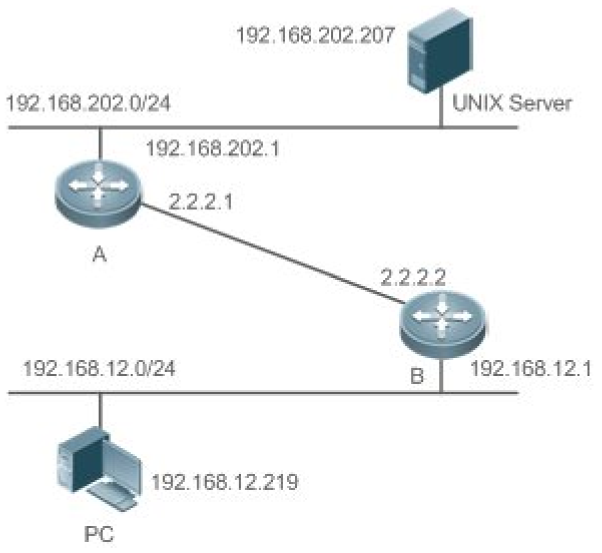
Typical Application	Scenario
Applying Time Range to an ACL	Apply a time range to an ACL module so that the time-based ACL takes effect

4.2.1 Applying Time Range to an ACL

Application Scenario

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

Figure 4-1



Note

Configure an ACL on device B to implement the following security function:

Hosts in network segment 192.168.12.0/24 can access the Telnet service on a remote Unix host during normal working hours only.

Functional Deployment

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

4.3 Function Details

Basic Concepts

- Absolute Time Range

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

- Periodic Time

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

Features

Feature	Function
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.

Related Configuration

- Configuring Time Range

No time range is configured by default.

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

- Configuring Absolute Time Range

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

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

4. 3. 2 Using Periodic Time

Working Principle

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

Related Configuration

- Configuring Time Range

No time range is configured by default.

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

- Configure Periodic Time

No periodic time is configured by default.

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

4.4 Configuration Details

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

❖ Configuring Absolute Time Range

Command	**absolute** { [**star**t *time date*] | [**end** *time date*] }
Parameter Description	**star**t *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	**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.

4.5 Monitoring and Maintaining Time Range

Displaying the Running Status

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

5. CONFIGURING USB

5.1 Overview

Universal serial bus (USB) is an external bus standard. In this document, USB refers to a USB-compliant peripheral device, for example, a USB flash drive.

USB is a hot swappable device. You can use it to copy files (such as configuration and log files) from a communication device, or copy external data (such as system upgrade files) to the flash of the communication device.

Specific application scenarios of the USB are detailed in configuration guides of related functions. This document describes only how to identify, use, and remove the USB and view information about the USB.

5.2 Applications

Application	Description
Using a USB Flash Drive to Upgrade a Device	Upgrade files are stored on a USB flash drive. After a device is powered on, the device detects the USB flash drive and runs the upgrade command to load the upgrade files. After loading is completed, the device is reset and runs the upgraded version.

5.2.1 Using a USB Flash Drive to Upgrade a Device

Scenario

Upgrade files are stored on a USB flash drive. After a device is powered on, the device detects the USB flash drive and runs the upgrade command to load the upgrade files. After loading is completed, the device is reset and runs the upgraded version. An example of the upgrade command is as follows:

upgrade usb0:/s12k-ppc_11.0(1B2)_20131025_main_install.bin

If the file is valid and execution of this command succeeds, the device will be automatically reset and run the upgraded version.

Deployment

- Use the prefix "usb0:/" to access USB 0. Run the **show usb** command to display information about the USB with the ID 0.
- Run the **upgrade** command to perform upgrade.

5.3 Features

❖ Using the USB

Insert a USB into the USB slot. The system automatically searches for the USB. After the USB is located, the driver module automatically initializes the driver of the USB. After initialization, the system automatically loads the file system on the USB. Later, the system can read or write this USB.

➢ If the system finds a USB and successfully loads the driver, the following information will be displayed:

```
*Jan  1 00:09:42: %USB 5 USB_DISK_FOUND: USB Disk <Mass Storage> has been inserted
to USB port 0!
*Jan  1 00:09:42: %USB 5 USB_DISK_PARTITION_MOUNT: Mount usb0(type:FAT32),size :
1050673152B(1002MB)
```

➢ "Mass Storage" indicates the name of the searched device, and "usb0:" indicates the first USB. "Size" indicates the size of the partition. For example, according to the preceding information displayed, the USB flash drive has a space of 1002 MB.

➢ "Size" indicates the size of the partition.

❖ Removing the USB

Use a command line interface (CLI) command to remove the USB first; otherwise, an error may occur if the system is currently using the USB.

➢ If the USB is successfully removed, the following information will be displayed:

```
OK, now you can pull out the device 0.
```

You can remove the USB only after the preceding information is displayed.

5.4 Configuration

Configuration	Description and Command	
Using a USB	Mandatory.	
	N/A	
Removing a USB	(Mandatory) It is used to remove a USB.	
	usb remove	Removes a USB.

5.4.1 Using a USB

Configuration Effect

After a USB is loaded, you can run the file system commands (such as **dir**, **copy**, and **del**) to perform operations on the USB.

Notes

- The Qtech General Operating System (QOS) is applicable only to devices (generally common USB flash drives) that support standard Small Computer System Interface (SCSI) commands. Other devices, such as the USB flash drive embedded in the USB network interface card (NIC) and USB flash drive with the virtual CD-ROM drive, cannot be used in the QOS. Some devices are configured with the function of converting a USB port to the serial port.
- The USB supports only the FAT file system. Other file systems on the USB must be formatted to the FAT file system on a PC before the USB can be used on a device.
- The QOS supports the hub. When a USB flash drive is inserted to a port on a hub, the access path becomes different. If the USB flash drive is inserted to a USB port on a device, the access path is **usbX:/**, where **X** indicates the device ID. You can run the **show usb** command to display this path. If the USB flash drive is inserted to a USB port through a hub, the access path is **usbX-Y:/**, where **X** indicates the device ID, and **Y** indicates the hub port ID. For example, **usb0-3:/** indicates port 3 on the hub that is connected to USB port 0 on the device.

Configuration Steps

❖ Identifying a USB

A USB can be directly inserted to the USB slot without a CLI operation.

❖ Using a USB

Perform the following operations to copy files from a USB to the flash:

- Run the **cd** command to enter the partition of the USB.
- Run the **copy** command to copy files on the USB to the flash on the device.
- Run the **dir** command to check whether the files are copied to the device.

- If the USB has multiple partitions, you can access only the first FAT partition on the device.
- The path of the USB does not contain any upper-level directory. After running the **cd usbX:** command to access a USB, you can run the **cd flash:** command to return to the flash file system.

Verification

Run the **show usb** command to display information about the USB inserted to the device.

Configuration Example

❖ Using a USB Flash Drive

Scenario	Standalone environment

Configuration Steps

- ➢ Insert the USB flash drive into the USB slot of the device.
- ➢ Run the **show usb** command on the device console.
- ➢ Copy the **config.txt** file from the USB flash drive to the flash on the device.

```
Qtech#show usb
Device: Mass Storage
ID: 0
URL prefix: usb0
Disk Partitions:
usb0(type:vfat)
Size:15789711360B(15789.7MB)
Available size:15789686784B(15789.6MB)
Qtech#
Qtech#
Qtech#dir usb0:/
Directory of usb0:/
   1  rwx           4  Tue Jan  1 00:00:00 1980  fac_test
   2  rwx           1  Mon Sep 30 13:15:48 2013  config.txt
2 files, 0 directories
15,789,711,360 bytes total (15,789,686,784 bytes free)
Qtech#
Qtech#
Qtech#copy usb0:/config.txt flash:/
Copying: !
Accessing usb0:/config.txt finished, 1 bytes prepared
Flushing data to flash:/config.txt...
Flush data done
Qtech#
Qtech#
```

Verification

- ➢ Check whether the **config.txt** file exists on the flash.

```
Qtech#
Qtech#dir flash:/
Directory of flash:/
   1 drw          160  Wed Mar 31 08:40:01 2010  at
```

```
  2 drwx             160  Thu Jan  1 00:00:11 1970  dm
  3 drwx             160  Thu Jan  1 00:00:05 1970  rep
  4 drwx             160  Mon Apr 26 03:42:00 2010  scc
  5 drwx             160  Wed Mar 31 08:39:52 2010  ssh
  6 drwx             224  Thu Jan  1 00:00:06 1970  var
  7 d                288  Sat May 29 06:07:45 2010  web
  8 drwx             160  Thu Jan  1 00:00:11 1970  addr
  9 drwx             160  Sat May 29 06:07:44 2010  cwmp
 10 drwx             784  Sat May 29 06:07:47 2010  sync
 11   w               92  Tue Feb  2 01:06:55 2010  config_vsu.dat
 12  rw              244  Sat Apr  3 04:56:52 2010  config.text
 13  rwx               1  Thu Jan  1 00:00:30 1970  .issu_state
 14  rw                0  Tue Feb  2 01:07:03 2010  ss_ds_debug.txt
 15  rw             8448  Thu Jan  1 00:01:41 1970  .shadow
 16  rwx             268  Thu Jan  1 00:01:41 1970  .pswdinfo
 17  rw                4  Tue May 25 09:12:01 2010  reload
 18 drwx             232  Wed Mar 31 08:40:00 2010  snpv4
 19 drwx            6104  Sat May 29 06:10:45 2010  .config
 20                    1  Thu Jan  1 00:04:51 1970  config.txt
 21 d                160  Thu Jan  1 00:00:12 1970  syslog
 22 drwx             160  Tue May 25 03:05:01 2010  upgrade_ram
 23 drwx             160  Tue Feb  2 01:06:54 2010  dm_vdu
 24  rwx              16  Thu Jan  1 00:01:41 1970  .username.data
9 files, 15 directories
5,095,424 bytes total (4,960,256 bytes free)
Qtech#
```

Common Errors

- Insert a USB flash drive that supports non-SCSI commands to the device.
- The USB does not use the FAT file system, and cannot be identified by the system.

5.4.2 Removing a USB

Configuration Effect

Remove the USB and ensure that the USB and the device are intact.

Notes

- Run the **usb remove** command before removing the USB; otherwise, a system error occurs.

Configuration Steps

Running the Remove Command

- Mandatory.
- Run the **usb remove** command before removing the USB.

Removing the USB

After the remove command is executed, remove the USB.

Verification

Run the **show usb** command to display information about the USB inserted to the device.

Related Commands

Removing a USB

Command	**usb remove** *device-id*
Parameter Description	*device-id*: Indicates the ID of the USB port on the device. You can run the **show usb** command to display this ID.
Command Mode	Privileged EXEC mode
Usage Guide	Before removing a USB, run the **usb remove** command; otherwise, an error occurs if the USB is in use. If the command is executed, related information will be displayed, and you can remove the USB. If the command execution fails, the USB is in use. In this case, do not remove the USB until it is not in use.

Configuration Example

Removing a USB

Scenario	Standalone environment
Configuration Steps	➢ Run the **show usb** command to display the ID of the USB. ➢ Run the **usb remove** command to remove the USB.

```
Qtech#show usb
Device: Mass Storage
ID: 0
URL prefix: usb0
Disk Partitions:
usb0(type:vfat)
Size:15789711360B(15789.7MB)
```

	`Available size:15789686784B(15789.6MB)`
	`Qtech#`
	`Qtech#`
	`Qtech#usb remove 0`
	`OK, now you can pull out the device 0.`

Verification	➢ Run the **show usb** command again to check whether the USB is removed. If the device with ID 0 is not displayed in output of the **show usb** command, the USB is removed.

	`Qtech#show usb`
	`Qtech#`

5.5 Monitoring

Displaying

Description	Command
Displays information about the inserted USB.	**show usb**

6. CONFIGURING UFT

6.1 Overview

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

Protocols and Standards

N/A

6.2 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.

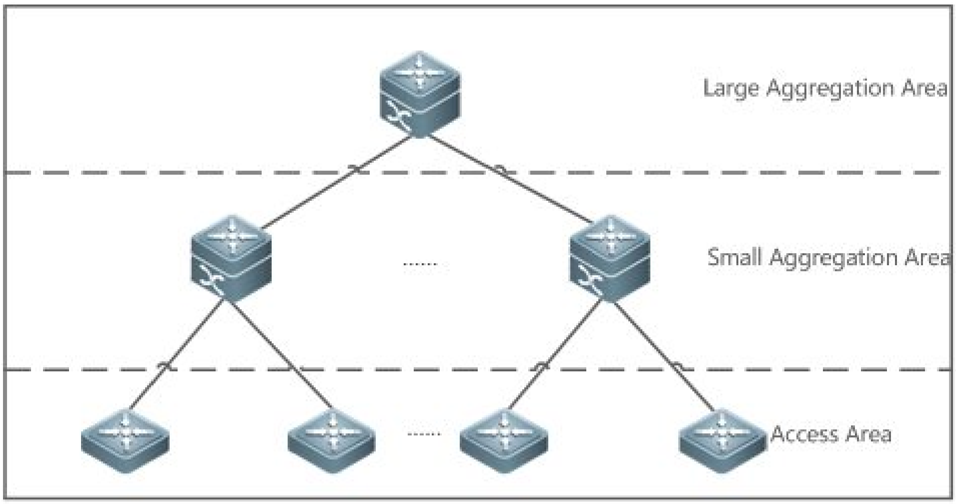
6.2.1 Dynamic Entry Allocation

Scenario

The following figure shows the simple and common topology of the campus network. The core device may be deployed in the small convergence area as a small convergence device. Layer 2 functions of the core device are mainly enabled. The core device can also be deployed in the large convergence area as a large convergence device. In this case, the core device works as a gateway. When the core device acts as a small convergence device, it requires a large enough size of the MAC address table.

Another application scenario of the core device is acting as a large convergence device, namely, a large gateway. Its access capability depends on the ARP and ND capacity, namely, the number of IPv4 and IPv6 terminals that can be accessed. Take the device installed with Windows7 operating system as an example. Such a device supports IPv4 and IPv6 dual-stack. When a terminal accesses the device, the terminal occupies one ARP entry and one ND entry. In this application scenario, a great number of ARP and ND entries are required.

Figure 6-1



Deployment

- Enable the switch to operate in Bridge mode of UFT to increase the MAC address table capacity.
- Enable the switch to operate in Gateway mode of UFT to increase the ARP and ND entry capacity.

6.3 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.

6.3.1 UFT Operating Mode

Working Principle

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

The UFT supports up to eight operating modes. The selected operating mode can take effect after it is saved and the device is restarted.

- Default

By default, the UFT mode of the switch is Default. In Default mode, each hardware entry of the switch is applied to most of application scenarios.

- ❖ Bridge

The Bridge mode is the Layer 2 forwarding mode. It is applied to the application scenarios in which pure Layer 2 services dominate. In Bridge mode, ARP,ND and MPLS capacity is greatly reduced and most of capacity is allocated to the MAC address table.

- ❖ Gateway

The Gateway mode is classified into three modes: gateway mode, gateway-max mode, and gateway-ndmax mode.

Gateway mode is applied to the application scenarios in which Layer 3 services dominate. Gateway-max mode is applied to the application scenarios in which a large number of terminals are deployed. Gateway-ndmax mode is applied to the application scenarios in which a large number of IPv6 terminals are deployed.

- ❖ Route

The Route mode is the network routing mode. It is applied to the application scenarios in which a great amount of routing and forwarding dominate.

The Route mode is classified into route-v4max and route-v6max modes. In these two modes, the IPv6 and IPv6 network routing table capacity are respectively allocated to maximum extent.

6.4 Configuration

Configuration Item	Suggestions and Related Commands	
Configuring UFT Operating Mode	Optional configuration. Switch over the current UFT operating mode of the switch.	
	switch-mode *mode_type* **slot** *slot_num*	Switches the UFT operating mode in stand-alone mode.
	switch-mode *mode_type* **switch** *switch_num* **slot** *slot_num*	Switches the UFT operating mode in VSU mode.

6.4.1 Configuring UFT Operating Mode

Configuration Effect

- Configure the Bridge mode to increase the Layer 2 entry size. The Bridge mode is applied to the application scenarios in which Layer 2 services dominate.
- Configure the Gateway mode to increase the ARP and ND table size. The Gateway mode is applied to the application scenarios in which Layer3 services dominate.
- Configure the Route mode to increase the routing table size. The Route mode is applied to the application scenarios that require a great amount of routing and forwarding.

Notes

- After configuration is complete, save it and restart the device to validate configuration.
- Change the UFT mode and save the change. When the device is restarted for the first time after being upgraded, The 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* **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. ➢ **bridge**: Bridge mode, which is applied to the application scenarios where pure Layer 2 services dominate. ➢ **gateway**: Gateway mode, which is applied to the application scenario in which Layer 3 services dominate. ➢ **gateway-max**: Gateway-max mode, which is applied to the application scenarios in which a large number of terminals are deployed. ➢ **gateway-ndmax**: Gateway-ndmax mode, which is applied to the application scenarios in which a large number of IPv6 terminals are deployed. ➢ **label**: Label mode, which is applied to the application scenarios that require a great amount of MPLS. ➢ **route-v4max**: IPv4 routing mode, which is applied to the application scenarios that require a great number of IPv4 routes. ➢ **route-v6max**: IPv6 routing mode, which is applied to the application scenarios that require a great number of IPv6 routes.

- Switching the UFT Operating Mode in VSU Mode

Mandatory configuration.

Use the **switch-mode** *mode_type* **switch** *switch_num* **slot** *slot_num* command to switch the UFT mode of the switch.

Command Syntax	**switch-mode** *mode_type* **switch** *switch_num* **slot** *slot_num*
Parameter Description	*mode_type*: UFT operating mode. *switch_num*: In stand-alone mode, the **switch** keyword is invisible. In VSU mode, the **switch** keyword indicates the chassis or box device. *slot_num*: indicates the line card installed in the chassis device.
Defaults	Default mode
Command Mode	Global configuration mode
Usage Guide	➢ In VSU mode, the line card can operate in the following modes: ➢ **default**: Default mode, which is applied to most of application scenarios. ➢ **bridge**: Bridge mode, which is applied to the application scenarios where pure Layer 2 services dominate. ➢ **gateway**: Gateway mode, which is applied to the application scenarios in which Layer 3 services dominate. ➢ **gateway-max**: Gateway-max mode, which is applied to the application scenarios in which a large number of terminals are deployed. ➢ **gateway-ndmax**: Gateway_ndmax mode, which is applied to the application scenarios in which a large number of IPv6 terminals are deployed. ➢ **label**: Label mode, which is applied to the application scenarios that require a great amount of MPLS. ➢ **route-v4max**: IPv4 routing mode, which is applied to the application scenarios that require a great number of IPv4 routes. ➢ **route-v6max**: IPv6 routing mode, which is applied to the application scenarios that require a great number of IPv6 routes.

Verification

- After the device is restarted, use the **show run** command to display the current line card status and check whether the configuration takes effect.
- Use the **show switch-mode status** command to display the UFT mode status.

Command Syntax	**show switch-mode status**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, interface configuration mode
Usage Guide	N/A

Configuration Example

```
Qtech(config)#show switch mode status
Slot No          Switch Mode
switch 1 slot 3     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 run
Building configuration...
Current configuration : 1366 bytes
version 11.0(1B2)
!
cwmp
!
install 3 M8600E 24XS4QXS DB
!
sysmac 1414.4b34.5624
!
nfpp
!
switch mode bridge slot 3
```

Check Method

Use the **show switch-mode status** command to display configuration information.

```
Qtech(config)#show switch mode status
Slot No          Switch Mode
3              bridge
```

Common Errors

-

6.5 Monitoring

Clearing

N/A

Displaying the Running Status

Function	Command
Displays UFT operating mode of the switch	**show switch-mode status**

Displaying Debugging Information

-

- The preceding monitoring and maintaining commands are also valid to the chassis devices and box devices, in stand-alone mode and VSU mode.
- In stand-alone mode, the **switch** keyword is invisible. For the chassis device, **slot** keyword indicates a specified line card.

7. CONFIGURING SUPERVISOR MODULE REDUNDANCY

7.1 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:

1. Improving the network availability

The supervisor module redundancy technology sustains data forwarding and the status information about user sessions during switching.

2. 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.

3. 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.

4. Preventing loss of user sessions

Thanks to real-time status synchronization, user sessions that are created prior to switching are not lost.

7.2 Applications

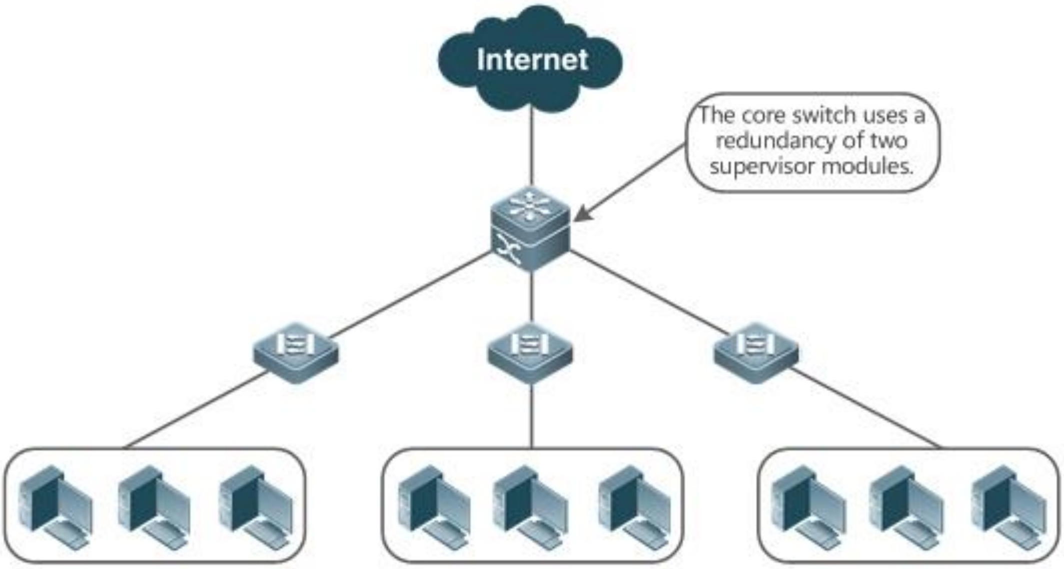
Application	Description
Redundancy of Supervisor Modules	On a core switch where two supervisor modules are installed, the redundancy technology can improve the network stability and system availability.

7.2.1 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 7-1


Internet
The core switch uses a redundancy of two supervisor modules.

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.

7.3 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.

7.3.1 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.

7.3.2 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:

5. The running-config file is synchronized when the device switches from the global configuration mode to privileged EXEC mode.
6. The startup-config file is synchronized when the **write** or **copy** command is executed to save the configuration.
7. 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.

7.4 Configuration

Configuration	Description and Command	
Configuring Manual Master/Slave Switching	Optional.	
	show redundancy states	Displays the hot backup status.
	redundancy forceswitch	Manually performs master/slave switching.
Configuring the Automatic Synchronization Interval	Optional.	
	redundancy	Enters the redundancy configuration mode.
	auto-sync time-period	Configures the automatic synchronization interval of configuration files in the case of redundancy of dual supervisor modules.
Resetting Supervisor Modules	Optional.	
	redundancy reload	Resets the slave supervisor module or resets both the master and slave supervisor modules at the same time.

7.4.1 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	Privileged EXEC mode

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`
	
	`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`
	
	`VSD staff redundancy state: realtime`

7.4.2 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: 3600 s`

7.4.3 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.

7.5 Monitoring

Displaying

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

8. CONFIGURING SYSLOG

8.1 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

8.2 Applications

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

8.2.1 Sending Syslogs to the Console

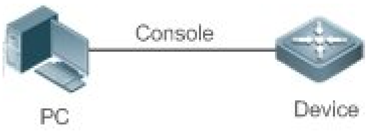
Scenario

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 8-1 shows the network topology.

Figure 8-1 Network topology



Deployment

Configure the device as follows:

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

8.2.2 Sending Syslogs to the Log Server

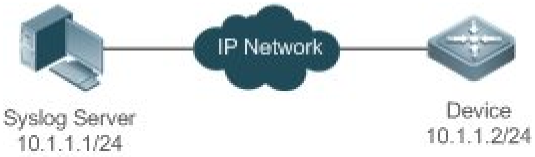
Scenario

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 8-2 shows the network topology.

Figure 8-2 Network topology



Deployment

Configure the device as follows:

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

8.3 Features

Basic Concepts

❖ Classification of Syslogs

Syslogs can be classified into two types:

- Log type
- Debug type

❖ Levels of Syslogs

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

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

The following table describes the log levels.

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

❖ Output Direction of Syslogs

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

The following table describes output directions of syslogs.

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

❖ RFC3164 Log Format

Formats of syslogs may vary with the syslog output direction.

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

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

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

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

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

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

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

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

The following describes each field in the log in details:

1. 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)

2. 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.

3. 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.

1. 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.

2. 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.

3. Level

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

4. 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.

5. Content

This field indicates the detailed content of the syslog.

Overview

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

8.3.1 Logging

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

Related Configuration

❖ Enable Logging

By default, logging is enabled.

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

❖ Enabling Log Redirection

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

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

❖ Enabling Log Statistics

By default, log statistics is disabled.

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

8.3.2 Syslog Format

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

Related Configuration

❖ Configuring the Timestamp Format

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

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

❖ Adding Sysname to the Syslog

By default, the syslog does not contain sysname.

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

❖ Adding the Sequence Number to the Syslog

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

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

❖ Enabling the Standard Log Format

By default, logs are displayed in the following format:

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

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

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

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

❖ Enabling the Private Log Format

By default, logs are displayed in the following format:

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

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

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

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

8.3.3 Logging Direction

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

Related Configuration

❖ Synchronizing User Input with Log Output

By default, this function is disabled.

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

❖ Configuring the Log Rate Limit

By default, no log rate limit is configured.

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

❖ Configuring the Log Redirection Rate Limit

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

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

❖ Configuring the Level of Logs Sent to the Console

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

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

❖ Sending Logs to the Monitor Terminal

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

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

❖ Configuring the Level of Logs Sent to the Monitor Terminal

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

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

❖ Writing Logs into the Memory Buffer

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

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

❖ Sending Logs to the Log Server

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

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

❖ Configuring the Level of Logs Sent to the Log Server

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

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

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

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

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

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

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

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

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

❖ Writing Logs into Log Files

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

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

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

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

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

❖ Configuring the Storage Time of Log Files

By default, the storage time is not configured.

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

❖ Immediately Writing Logs in the Buffer into Log Files

By default, 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.

8.3.4 Syslog Filtering

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

Working Principle

- Filtering Direction

Five log filtering directions are defined:

- **buffer**: Filters out logs sent to the log buffer, that is, logs displayed by the **show logging** command.
- **file**: Filters out logs written into log files.
- **server**: Filters out logs sent to the log server.
- **terminal**: Filters out logs sent to the Console and monitor terminal (including Telnet and SSH).

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

- Filtering Mode

Two filtering modes are available:

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

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

- Filter Rule

Two filtering rules are available:

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

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

Related Configuration

- Configuring the Log Filtering Direction

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

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

- Configuring the Log Filtering Mode

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

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

- Configuring the Log Filtering Rule

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

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

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

8.3.5 Syslog Monitoring

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

Working Principle

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

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

Related Configuration

- Enabling Logging of Login or Exit Attempts

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

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

- Enabling Logging of Operations

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

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

8.4 Configuration

Configuration	Description and Command	
Configuring Syslog Format	(Optional) It is used to configure the syslog format.	
	service timestamps [*message-type* [**uptime**| **datetime** [**msec**] [**year**]]]	Configures the timestamp format of syslogs.
	service sysname	Adds the sysname to the syslog.
	service sequence-numbers	Adds the sequence number to the syslog.
	service standard-syslog	Enables the standard syslog format.
	service private-syslog	Enables the private syslog format.
Sending Syslogs to the Console	(Optional) It is used to configure parameters for sending syslogs to the Console.	
	logging on	Enables logging.
	logging count	Enables log statistics.
	logging console [*level*]	Configures the level of logs displayed on the Console.
	logging rate-limit { *number* | **all** *number* | **console** {*number* | **all** *number* } } [**except** [*severity*]]	Configures the log rate limit.
Sending Syslogs to the Monitor Terminal	(Optional) It is used to configure parameters for sending syslogs to the monitor terminal.	
	terminal monitor	Enables the monitor terminal to display logs.
	logging monitor [*level*]	Configures the level of logs displayed on the monitor terminal.
Writing Syslogs into the Memory Buffer	(Optional) It is used to configure parameters for writing syslogs into the memory buffer.	
	logging buffered [*buffer-size*] [*level*]	Configures parameters for writing syslogs into the memory buffer, including the buffer size and log level.
Sending Syslogs to the Log Server	(Optional) It is used to configure parameters for sending syslogs to the log server.	
	logging server [**oob**] { *ip-address* | **ipv6** *ipv6-address* } [**via** *mgmt-name*] [**udp-port** *port*] [**vrf** *vrf-name*]	Sends logs to a specified log server.

Configuration	Description and Command	
	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 { **flash:***filename* | **usb0**:*filename* | **usb1**:*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 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 Syslog Redirection	(Optional) It is used to enable the log redirection function.	
	logging rd on	Enables the log redirection function.
	logging rd rate-limit *number* [**except** *severity*]	Configures the log redirection rate limit.
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.

8.4.1 Configuring Syslog Format

Configuration Effect

- ➢ Configure the format of syslogs.

Notes

❖ RFC3164 Log Format

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

Configuration Steps

❖ Configuring the Timestamp Format of Syslogs

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

❖ Adding the Sysname to the Syslog

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

❖ Adding the Sequence Number to the Syslog

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

❖ Enabling the Standard Log Format

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

❖ Enabling the Private Log Format

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

Verification

- ➢ Generate a syslog, and check the log format.

Related Commands

❖ Configuring the Timestamp Format of Syslogs

Command	**service timestamps** [*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.

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
```

8.4.2 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)#show logging config`
	`Syslog logging: enabled`
	`  Console logging: level informational, 1303 messages logged`
	`  Monitor logging: level debugging, 0 messages logged`
	`  Buffer logging: level debugging, 1303 messages logged`
	`  File logging: level informational, 118 messages logged`
	`  File name:syslog_test.txt, size 128 Kbytes, have written 5 files`

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.

	`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`

8.4.3 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.

8.4.4 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`

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.

	`  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`
	`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.

8.4.5 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* } [**via** *mgmt-name*] [**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.

	via *mgmt-name*: Specifies the MGMT interface used by the log server when the **oob** option is included in the command. **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 specify **via** only when **oob** is included in the command. In this case, **vrf** cannot be used. You can configure up to five log servers on a Qtech product.

❖ Configuring the Level of Logs Sent to the Log Server

Command	**logging trap** [*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

<table>
<tr><td><b>Scenario</b></td><td>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.</td></tr>
<tr><td></td><td></td></tr>
<tr><td><b>Configuration Steps</b></td><td>➢ Configure parameters for sending syslogs to the log server.</td></tr>
<tr><td></td><td><pre>
Qtech# configure terminal
Qtech(config)# logging server 10.1.1.100
Qtech(config)# logging trap debugging
Qtech(config)# logging source interface Loopback 0
</pre></td></tr>
<tr><td></td><td></td></tr>
<tr><td><b>Verification</b></td><td>➢ Run the <b>show logging config</b> command to display the configuration.</td></tr>
<tr><td></td><td><pre>
Qtech#show logging config
Syslog logging: enabled
  Console logging: level informational, 1307 messages logged
  Monitor logging: level informational, 0 messages logged
  Buffer logging: level informational, 1307 messages logged
  File logging: level informational, 122 messages logged
  File name:syslog_test.txt, size 128 Kbytes, have written 5 files
  Standard format:false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
</pre></td></tr>
</table>

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.

	`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`

8.4.6 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 Interval at Which Logs Are Written into Log Files

- ➢ (Optional) By default, syslogs are written to log files every hour.
- ➢ Unless otherwise specified, perform this configuration on the device to configure the interval at which logs are written into log files.

- ❖ Configuring the Storage Time of Log Files

- (Optional) By default, no storage time is configured.
- Unless otherwise specified, perform this configuration on the device to configure the storage time of log files.

- ❖ Immediately Writing Logs in the Buffer into Log Files

- (Optional) By default, syslogs are stored in the buffer and then written into log files periodically or when the buffer is full.
- Unless otherwise specified, perform this configuration to write logs in the buffer into log files immediately. This command takes effect only once after it is configured.

Verification

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

Related Commands

- ❖ Writing Logs into Log Files

Command	**logging file** { **flash:***filename* | **usb0**:*filename* | **usb1**:*filename* } [*max-file-size*] [*level*]
Parameter Description	**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. **usb1**: Indicates that log files will be stored on USB 1. This option is supported only when the device has two USB ports and USB flash drives are inserted into the USB ports. *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 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`
	`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`

8.4.7 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
Configuratio	Log filtering modes include contains-only and filter-only. The default filtering mode is filter-only.

n Usage	

❖ 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 Usage	Log filtering rules include exact-match and single-match. 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`

8.4.8 Configuring Syslog Redirection

Configuration Effect

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

- On a card-type VSU, after the log redirection function is enabled, logs on the secondary or standby supervisor module will be redirected to the active supervisor module, and the role flag "(device ID/supervisor module name) will be added to each log to indicate that the log is redirected. If four supervisor modules form a VSU, the role flags are listed as follows: (*1/M1), (*1/M2), (*2/M1), and (*2/M2).

Notes

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

Configuration Steps

- Enabling Log Redirection

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

- Configuring the Rate Limit

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

Verification

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

Related Commands

- Enabling Log Redirection

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

- Configuring the Rate Limit

Command	**logging rd rate-limit** *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`

8.4.9 Configuring Syslog Monitoring

Configuration Effect

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

Notes

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

Configuration Steps

- Enabling Logging of Login/Exit Attempts

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

- Enabling logging of Operations

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

Verification

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

Related Commands

- Enabling Logging of Login/Exit Attempts

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

- Enabling Logging of Operations

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

Configuration Example

- Configuring Syslog Monitoring

Scenario	It is required to configure the syslog monitoring function as follows: 1. Enable logging of login/exit attempts. 2. Enable logging of operations.
Configuration Steps	➢ Configure the syslog monitoring function.

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

8.4.10 Synchronizing User Input with Log Output

Configuration Effect

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

Notes

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

Configuration Steps

❖ Synchronizing User Input with Log Output

➢ (Optional) By default, the synchronization function is disabled.

➢ Unless otherwise specified, perform this configuration on every line to synchronize user input with log output.

Verification

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

Related Commands

- ❖ Synchronizing User Input with Log Output

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

Configuration Example

- ❖ Synchronizing User Input with Log Output

Scenario	It is required to synchronize the user input with log output as follows: 1. Enable the synchronization function.
Configuration Steps	➢ Configure the synchronization function.

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

8.5 Monitoring

Clearing

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

Description	Command
Clears logs in the memory buffer.	**clear logging**

Displaying

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

9. CONFIGURING MONITOR

9.1 Overview

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

- Automatic fan speed adjustment based on ambient temperature changes
- Real-time temperature monitoring of boards to alert users

By default, the intelligent monitoring function is enabled after the device is powered on. It does not require any manual configuration.

Protocol Specification

N/A

9.2 Features

Basic Concepts

N/A

Features

Feature	Function
Intelligent Speed Adjustment of Fans	The rotating speed of fans is automatically adjusted as the temperature changes to address the heat dissipation needs of the system.
Intelligent Temperature Monitoring	The system automatically monitors the temperature. When the temperature exceeds a certain threshold, the system automatically generates an alarm.
Power monitoring	The system automatically monitors the power. When the power is insufficient or cannot be identified, the system automatically generates an alarm.

9.2.1 Intelligent Speed Adjustment of Fans

As the ambient temperature rises or drops, the fans automatically raise or reduce their rotating speed to dissipate heat and ensure that the noise is low.

Working Principle

Verification

- Run the **show fan** command to display working status of all fans.
- Run the **show fan speed command** to display rotating speed.

9.2.2 Intelligent Temperature Monitoring

The system automatically monitors the temperature. When the temperature changes, the system automatically notifies users.

Working Principle

The system monitors the temperature once per minute. When the temperature exceeds a certain threshold, the system takes a certain action. The temperature and action vary with different devices.

Verification

Run the **show temperature** command to display system temperature.

9.2.3 Power Monitoring

The system automatically monitors the power. When the power is insufficient or cannot be identified, the system automatically generates an alarm.

Working Principle

The system monitors the power once per minutes. If the system finds the power insufficient, the alarm LED becomes yellow and a Syslog message is generated. Once the alarm event is resolved, the system recovers. If the system cannot identify the inserted power, the alarm LED becomes yellow. After you remove the power, the system recovers.

Verification

Run the **show power** command to display power information.

10. CONFIGURING PKG_MGMT

10.1 Overview

Package management (pkg_mgmt) is a package management and upgrade module. This module is responsible for installing, upgrading/degrading, querying and maintaining various components of the device, among which upgrade is the main function. Through upgrade, users can install new version of software that is more stable or powerful. Adopting a modular structure, the QOS system supports overall upgrade.

✓ This document is for only version 11.0 and later, excluding those upgraded from earlier versions.

Protocols and Standards

N/A

10.2 Applications

Application	Scenario
Upgrading/Degrading Subsystem	Upgrade subsystem firmware like boot, kernel, and rootfs on the device.
Upgrading/Degrading a Single Feature Package	Upgrade a single feature package on the device.
Installing a Hot Patch Package	Install a hot patch, and repair a certain part of the feature component.
Auto-Sync for Upgrade	Configure the auto sync policy, range and path.

10.2.1 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 or SD card, connect the USB flash drive to the device, and then run an upgrade command to upgrade the package.

You must store the rack package in a USB flash drive before performing the upgrade because the rack package is too large to be stored in the memory space of the device.

10.2.2 Upgrading Subsystem by One-click

Scenario

Upgrade the firmware automatically without interrupting services on a dual-device VSU system. While either in VSU mode or in standalone mode, one single device will restart after this configuration, thus interrupting services.

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 or SD card, connect the USB flash drive or SD card to the device, and then run an upgrade command to upgrade the package.

10.2.3 Installing a Hot Patch Package

Scenario

To fix software bugs without restarting the device, you can install hot patch packages. Hot patch packages are only applicable to fixing a specific software version. Generally, hot patch packages are released to fix the software of a certain version only when the device cannot be started in the user's environment.

The most significant feature of hot patch upgrade is that all bugs can be fixed without device restart after the upgrade is completed.

Deployment

You can store this package in the root directory of the TFTP server, download the package to the local device, and then complete the upgrade. You can also store the package in a USB flash drive or SD card, connect the USB flash drive or SD card to the device, and then complete the upgrade.

10.3 Features

Basic Concepts

↘ Subsystem

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

- boot: After being powered on, the device loads and runs the boot subsystem first. This subsystem is responsible for initializing the device, and loading and running system images.

- kernel: kernel is the OS core part of the system. This subsystem shields hardware composition of the system and provides applications with abstract running environment.
- rootfs: rootfs is the collection of applications in the system.

↘ Main 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 boot, kernel, and rootfs subsystems. The main package can be used for overall system upgrade/degradation.

Overview

Feature	Description
Upgrading/Degrading and Managing Subsystem Components	Upgrades/degrades a subsystem.

10.3.1 Upgrading/Degrading and Managing Subsystem Components

Subsystem upgrade/degradation aims to upgrade the software by replacing the subsystem components of the device with the subsystem components in the firmware. The subsystem component contains redundancy design. Subsystems of the device are not directly replaced with the subsystems in the package during upgrade/degradation in most cases. Instead, subsystems are added to the device and then activated during upgrade/degradation.

Working Principle

↘ Upgrade/Degradation

Various subsystems exist on the device in different forms. Therefore, upgrade/degradation varies with different subsystems.

- boot: Generally, this subsystem exists on the norflash device in the form of images. Therefore, upgrading/degrading this subsystem is to write the image into the norflash device.
- kernel: This subsystem exists in a specific partition in the form of files. Therefore, upgrading/degrading this subsystem is to write the file.
- rootfs: Generally, this subsystem exists on the nandflash device in the form of images. Therefore, upgrading/degrading this subsystem is to write the image into the nandflash device.

↘ Management

Query the subsystem components that are available currently and then load subsystem components as required.

Each subsystem component contains redundancy design. During the upgrade/degradation:

- boot: The boot subsystem always contains a master boot subsystem and a slave boot subsystem. Only the master boot subsystem is involved in the upgrade, and the slave boot subsystem serves as the redundancy backup all along.
- kernel: as the kernel subsystem contains at least one redundancy backup. More redundancy backups are allowed if there is enough space.
- rootfs: The rootfs subsystem always contains a redundancy backup.

The boot component is not included in the scope of subsystem management due to its particularity. During upgrade of the kernel or rootfs subsystem component, the upgrade/degradation module always records the subsystem component in use, the redundant subsystem component, and management information about various versions.

Relevant Configuration

↘ Upgrade

- Store the upgrade file on the local device, and then run the **upgrade** command for upgrade.

10.3.2 Upgrading/Degrading and Managing Hot Patch Packages

Working Principle

In fact, upgrading a feature component is replacing feature files on the device with the feature files in the package.

Upgrading hot patch packages is similar to upgrading features. The difference is that only files to be revised are replaced during hot patch package upgrade. In addition, after the files are replaced, the new files take effect automatically.

After package upgrade, component upgrade cannot be performed.

↘ Management

Similar to feature component management, hot patch management also includes the query, installation, and uninstallation operation, which is the result of adding, querying and deleting data respectively.

Hot patches and feature components are managed based on the same technology. The difference is that the hot patches involve three different states, that is, Not installed, Installed, and Activated. These states are described as follows:

The hot patch in Installed state only indicates that this hot patch exists on the device, but it has not taken effect yet.

Only the hot patch in Activated state is valid.

Relevant Configuration

↘ Upgrade

- Store the upgrade file in the local file system, and then run the **upgrade** command for upgrade.

- Activating a Hot Patch

- You can run the **patch active** command to activate a patch temporarily. The patch becomes invalid after device restart. To use this patch after device restart, you need to activate it again.
- You can also run the **patch running** command to activate a patch already permanently. The patch is still valid after device start.
- The patch not activated will never become valid.

- Deactivating a Hot Patch

- To deactivate an activated patch, run the **patch deactive** command.

- Uninstalling a Hot Patch

- You can run the **patch delete** command to uninstall a hot patch.

10.4 Configuration

Configuration	Description and Command	
Upgrading/Degrading a Firmware	⚠ The basic function of the configuration is installing and upgrading/degrading a subsystem firmware, feature package, and hot patch package. This command is valid on both the box-type device and rack-type device.	
	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* [**force**]	*path* is the path of the firmware on the server. This command is used to download afirmware from the server and upgrade the package automatically.

	upgrade download oob_tftp://*path* [**force**]	*path* is the path of the firmware on the server. **via mgmt** *number*: If the transfer mode is *oob_tftp* and there are multiple MGMT ports, you can select a specific port. This command is used to download afirmware from the server and upgrade the package automatically.
	patch active	Activates a patch temporarily.
	patch running	Activates a patch permanently,
Deactivating and Uninstalling a Hot Patch	(Optional) Deactivates or uninstalls a hot patch.	
	patch delete	Uninstalls a hot patch.

10.4.1 Upgrading/Degrading a Firmware

Configuration Effect

Available firmwares include the main package.

- 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

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 component, you can run the **show upgrade history** command to check whether the upgrade is successful.
- After upgrading a hot patch package, you can run the **show patch** command to check whether the upgrade is successful.

Commands

Upgrade

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

Command	**upgrade download tftp:***/path* [**force**] **upgrade download oob_tftp:***/path* [**force**]
Parameter Description	*url* indicates the path of the firmware in the device file system. **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 History

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

Displaying the Feature Components Already Installed

Command	**show component** [*component _name*]
Parameter Description	[*component _name*]: component name When this parameter value is N/A, the command is used to display all components already installed on the device and basic information of these components. When this parameter value is not N/A, the command is used to display detailed information of the corresponding component, check whether the component is intact, and check whether this component works properly.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuration Example

↘ Example of Upgrading a Subsystem Firmware 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.** ● **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 or SD card.**
Configuration Steps	● Run the upgrade command. ● After upgrading the subsystem, restart the device.

	`Qtech# upgrade download`
	`tftp://192.168.201.98/eg1000m_main_1.0.0.0f328e91.bin`
	`Accessing`
	`tftp://192.168.201.98/eg1000m_main_1.0.0.0f328e91.bin...`
	`!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!`
	`!!!!!!!!!!!!!!!`
	`!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!`
	`!!!!!!!!!!!!!!!`
	`!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!`

```
!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!
Transmission finished, file length 21525888 bytes.
Upgrade processing is 10%
 Upgrade processing is 60%
 Upgrade processing is 90%

 Upgrade info [OK]
         Kernel version[2.6.32.91f9d21 >2.6.32.9f8b56f]
         Rootfs version[1.0.0.2ad02537 >1.0.0.1bcc12e8]
 Upgrade processing is 100%
 Reload system to take effect!
Reload system?(Y/N)y
 Restarting system.
```

Verification	- Check the system version on the current device. If the version information changes, the upgrade is successful.

```
QSW-6510-54F#show version
System description        : QTECH Full 10G Routing Switch(QSW-6510-54F)
System start time         : 2017-09-28 16:15:55
System uptime             : 3:23:24:09
System hardware version : 1.10
System software version : QSW-6510_OS 11.0_8_1, Release(04192412)
System patch number       : NA
System serial number      : G1K80M9001642
System boot version       : 1.2.19
Module information:
  Slot 0 : QSW-6510-54F
    Hardware version      : 1.10
    System start time     : 2017-09-29 00:09:58
    Boot version          : 1.2.19
    Software version      : QSW-6510_OS 11.0_8_1, Release(04192412)
    Serial number         : G1K80M9001642
```

Example of Installing a Patch Package 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.** ● **Copy the firmware to a USB flash drive, connect the USB flash drive to the device, and then run the upgrade *url* command to upgrade the firmware in the USB flash drive.**
Configuration Steps	● Run the upgrade command. ● Activate the hot patch.

```
Qtech#upgrade download
tftp://192.168.201.98/eg1000m QOS11.0(1C2)_20131008_patch
.bin
Accessing
tftp://192.168.201.98/eg1000m QOS11.0(1C2)_20131008_patch
.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!
Transmission finished, file length 9868 bytes.
Upgrade processing is 10%
 Upgrade processing is 60%

 Upgrade info [OK]
   patch_bridge version[1.0.0.1952]
 Upgrade processing is 90%


 Upgrade info [OK]
   patch_install version[1.0.0.192e35a]
Qtech#patch running
 The patch on the system now is in running status
```

Verification	● Check the hot patches installed on the current device.

```
:patch package patch_install installed in the system,
version:pa1
 Package : patch_bridge

 Status：running

 Version: pa1        Build time: Mon May 13 09:03:07 2013
     Size: 277       Install time: Tue May 21 03:07:17 2013
     Description: a patch for bridge
     Required packages: None
```

Common Errors

If an error occurs during the upgrade, the upgrade module displays an error message. The following provides an example:

```
Upgrade info [ERR]
      Reason:creat config file err(217)
```

The following describes several types of common error messages:

- Invalid firmware: The cause is that the firmware may be damaged or incorrect. It is recommended to obtain the firmware again and perform the upgrade operation.
- Firmware not supported by the device: The cause is that you may use the firmware of other devices by mistake. It is recommended to obtain the firmware again, verify the package, and perform the upgrade operation.
- Insufficient device space: Generally, this error occurs on a rack-type device. It is recommended to check whether the device is supplied with a USB flash drive or SD card. Generally, this device has a USB flash drive.

10.4.2 Deactivating and Uninstalling a Hot Patch

Configuration Effect

An activated hot patch is deactivated or uninstalled.

Notes

A hot patch that is not activated does not take effect; therefore, you cannot deactivate it.

Configuration Steps

- Deactivating an Activated Patch
- Optional configuration. To deactivate an activated patch, run the **patch deactive** command.
- Uninstalling a Hot Patch
- Optional configuration. To uninstall a hot patch already installed, run the **patch delete** command.

Verification

- You can run the **show patch** command to check whether a patch is activated or uninstalled.

Commands

- Deleting a Hot Patch

Command	**patch delete**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	This command is used to remove the hot patch package from the device.

Configuration Example

- Deactivating and Uninstalling a Patch on the Box Device

Configuration Steps	● **Run the patch deactivation command.** ● **Run the patch deletion command.**

	`Qtech#patch deactive`
	`Deactive the patch package success`
	`Qtech# patch delete`
	`Clear the patch patch_bridge success`
	`Clear the patch success`

Verification	● Display patch status.

	`Qtech#show patch`
	`No patch package installed in the system`

Common Errors

- ➢ Run the **patch deactive** command when the patch is not activated. It is recommended to check the patch status. You can run the **patch deactive** command only when the patch is in the **status:running** state.

10.5 Monitoring

Clearing

Function	Command
Deletes a hot patch package already installed.	**patch delete** [**slot** { *num* **| M1 | M2 | all** }]

Displaying

Function	Command
Displays all components already installed on the current device and their information.	**show component** [*component _name*]
Displays the upgrade history.	**show upgrade history**

11. CONFIGURING OPENFLOW

11.1 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

11.2 Typical Application

Typical Application	Scenario
Centralized Control	Perform centralized management of authentication.

11.2.1 Centralized Control

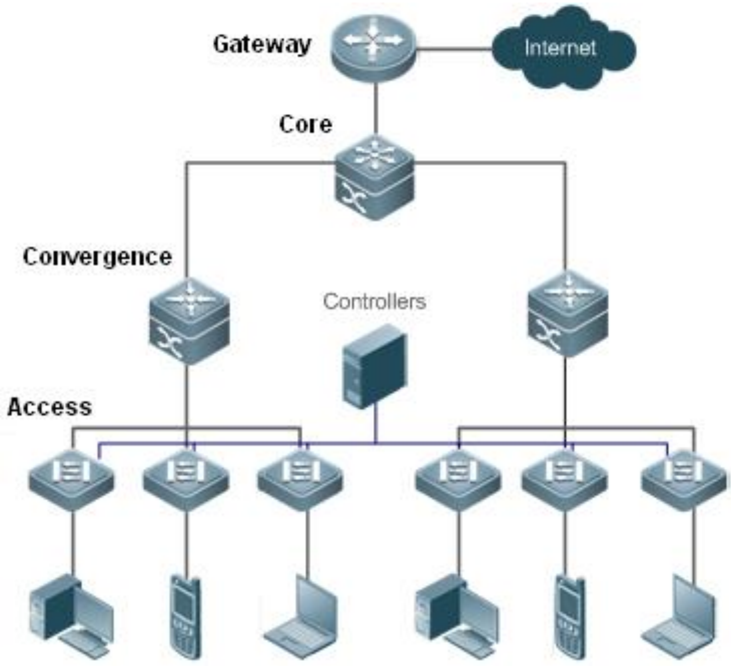
Application Scenario

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 11-1



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.

11.3 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.
STP Control	Set whether STP management is performed by a Software Defined Network (SDN) controller or the local device.

11.3.1 Separating Control from Forwarding

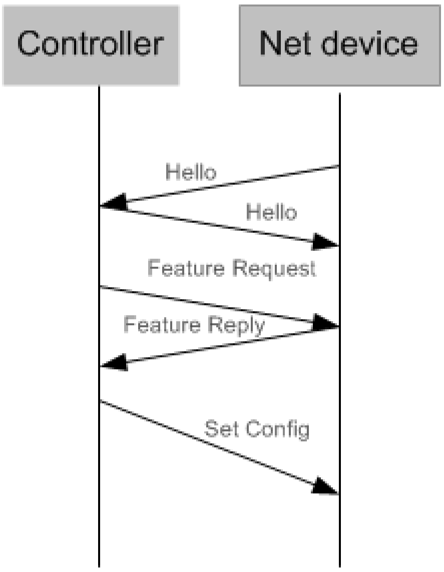
Perform centralized management of the network control plane, so that the entire network is centrally managed at ease (as compared with the status quo of the network), thereby reducing maintenance and management costs.

Working Principle

The OpenFlow protocol runs over Transport Layer Security (TLS) or unprotected TCP connections, and defines the interaction between the controller and network devices. The controller sends flow table information to the network devices, so as to control the method for forwarding network data packets and some configuration parameters. Each network device will send a notification message to the controller when its link is interrupted or when the network device receives a data packet in which no forwarding action has been specified. In this way, the interaction between the controller and the network devices is implemented to eventually control the transmission of the entire network.

The process of discovering each other shall be completed before the controller and a network device interact with each other. Figure 11-2 shows the specific actions involved in this process.

Figure 11 2



Hello packets are sent between the controller and the network device to achieve a handshake. When the handshake is done, the controller requests specific information about the network device, including (but not limited to) the number of ports on the network device and the capability of each port (such as the Feature Request/Reply shown in Figure 11-2). Then the controller delivers specific user configurations (such as Set Config shown in Figure 11-2) to the network device. After a connection is established, the controller defines various flows and corresponding actions for the flows, and delivers them in a flow table to the network device. When a data packet enters the network device, the network device matches the data packet with the flow table according to present flow table rules and performs a corresponding action (including forwarding, discarding, and modifying the packet). At the same time, a corresponding counter is updated. If no match is found in the flow table, the network device forwards the data packet to the controller.

The network device locally maintains the flow table delivered from the controller. If the data packet to be forwarded is already defined in the flow table, the network device directly forwards the data packet. Otherwise, the data packet is sent to the controller to confirm the transmission path (which can be understood as control plane parsing to generate the flow table) and then forwarded based on the flow table delivered from the controller.

Related Configuration

❖ Default Configuration

The OpenFlow protocol is disabled by default.

❖ Enabling/Disabling OpenFlow to Connect/Disconnect the Controller

➢ Run the **of controller-ip** command to enable OpenFlow.

➢ Run the **no of controller-ip** command to disable OpenFlow.

11.3.2 STP Control

According to the OpenFlow protocol, the Spanning Tree Protocol (STP) function of a network device allows the network device to be managed either locally or through an SDN controller. Therefore, a configuration command is required to perform switching between the two management methods. The configuration command takes effect only when OpenFlow management is enabled.

If loop control is enabled on the controller, do not enable the STP function on a network device; otherwise, the two functions conflict with each other. Enable the STP function on the network device only when loop control is disabled on the controller and a loop probably exists in the network device. After the STP function is enabled on the network device, STP configuration is further required on the network device. For details, see the section about STP configuration.

Working Principle

A network device communicates with the controller using the OFPC-STP field that is carried in an OFPT_FEATURES_REPLY message of the OpenFlow protocol to decide which subject will currently perform STP management. When the controller performs STP management according to the configuration, all STP-related processing is performed by the controller; otherwise, the network device itself performs the processing in a conventional way.

Related Configuration

❖ Default Configuration

The STP function is provided by the controller by default.

❖ Enabling STP Management on the SDN Controller or Local Device

➢ Run the **of stp** command to set STP management performed by the SDN controller.

➢ Run the **no of stp** command to set STP management performed by the local network device.

11.4 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 STP	Optional configuration, which is used to enable the STP function of the SDN controller as necessary.	
	of stp	Enables the STP management function on the SDN controller.
	no of stp	Enables the STP management function on the local device.

11.4.1 Configuring OpenFlow

Configuration Effect

- Trigger the network device to establish a connection with the specified controller and eventually establish an OpenFlow management channel.

Notes

- Before switching the address of the controller, disable and then enable the OpenFlow function again.

Configuration Method

- Enabling the OpenFlow Function
- This configuration is required for enabling OpenFlow.
- Disabling the OpenFlow Function
- This configuration is required for switching the controller or disabling the OpenFlow function.
- Displaying the Connection Status Between the OpenFlow Device and the Controller
- Display the connection status between the current device and the controller.

Verification

- Display the connection status of current protocol using the **show of** command.

Related Commands

- Enabling the OpenFlow Function

Command	**of controller-ip** ***ip-address*** [**port** *port-value*] **interface** [*interface-id*]
Parameter Description	**controller-ip** ***ip-address***: controller IP address. **port** *port-value*: port that connects to the controller. The default value is 6633. **Interface** *interface-id*: port ID, which can be either an out-of-band management interface or a common in-band physical Ethernet interface.
Command Mode	Global configuration mode
Usage Guide	-

- Disabling the OpenFlow Function

Command	**no of controller-ip**
Parameter Description	**-**

Command Mode	Global configuration mode
Usage Guide	Run this command before switching the controller.

❖ Enabling or Disabling the Local STP Function on the OpenFlow Device

Command	**of stp**
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	Run this command to select enabling the local STP function on the network device or enabling the STP function on the OpenFlow controller.

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

Command	**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

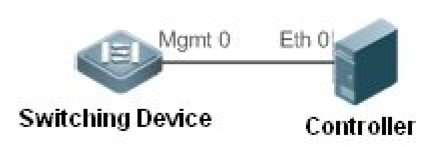
Command	**show of port**
Parameter Description	-

Command Mode	Global configuration mode
Usage Guide	-

Configuration Examples

❖ Configuring the IP Address and Access Port (6633 by Default) of the Controller to Connect the Network Device

Network Environment Figure 11-3



Configuration Method

➢ Enable the OpenFlow function on the network device and specify the controller IP address.

```
Qtech# configure terminal
Qtech(config)# interface mgmt 0
Qtech(config if)# ip address 172.18.2.36 255.255.255.0
Qtech(config if)# exit
Qtech(config)# of controller ip 172.18.2.35 interface mgmt 0
```

or

```
Qtech(config)# of controller ip 172.18.2.35 port 6633 interface mgmt 0
```

Verification

➢ Display the connection status between the OpenFlow device and the controller, port status and flow table status.

```
Qtech# show of
Controller is 172.18.2.35 port 6633,connected.
Qtech#show of port
STP is controlled by SDN Controller.
    PORTID    IFX     COFIG      STATE      LINK    SPEED    DUPLEX
       1    1     0x0000   0x0001     0      0        0
       2    2     0x0000   0x0001     0      0        0
       3    3     0x0000   0x0001     0      0       0
       4    4     0x0000   0x0001     0      0       0
       5    5     0x0000   0x0001     0      0       0
       6    6     0x0000   0x0001     0      0       0
       7    7     0x0000   0x0001     0      0       0
       8    8     0x0000   0x0001     0      0       0
       9    9     0x0000   0x0001     0      0       0
      10   10    0x0000   0x0001     0      0       0
      11   11    0x0000   0x0001     0      0       0
      12   12    0x0000   0x0001     0      0       0
      13   13    0x0000   0x0001     0      0       0
      14   14    0x0000   0x0001     0      0       0
      15   15    0x0000   0x0001     0      0       0
      16   16    0x0000   0x0001     0      0       0

Qtech#show of flowtable
openflow flow count = 1
****************************FLOW START*******************************
KEY:
          SMAC                   DMAC               SIP
DIP
   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*********************************
```

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.

11.4.2 Configuring OpenFlow STP

Configuration Effect

- ➢ Enable the STP function on the SDN controller or the STP function on the local device, so that the SDN controller or local device performs STP processing.

Notes

- ➢ The configuration is effective only during the next connection to the controller after the OpenFlow function is enabled.

Configuration Method

- ❖ Enabling the STP Function on the OpenFlow Device
- ➢ Mandatory configuration. The STP function is enabled on the SDN controller by default.
- ❖ Enabling STP Management on the SDN Controller
- ➢ Default configuration.
- ❖ Displaying Current Configuration
- ➢ Display the current port status.

Verification

- ➢ Display current configuration using the **show of port** command.

Related Commands

- ❖ Enabling or Disabling the Local STP Function on the OpenFlow Device

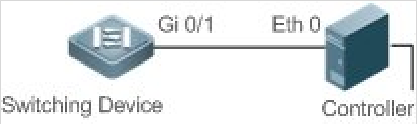
Command	[**no**] **of stp**
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	Run this command to select enabling the local STP function on the network device or enabling the STP function on the OpenFlow controller.

❖ Displaying Port Information About the OpenFlow Device

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

Configuration Examples

❖ Enabling Local STP or STP of OpenFlow

Network Environment **Figure 11-4**	

Configuration Method	■ Enable STP of OpenFlow.
	`Qtech(config)#of stp`
	■ Enable local STP.
	`Qtech(config)#no of stp`

Verification

- Display STP status of the OpenFlow device.

```
Qtech(config)#of stp
Qtech(config)#show of port
STP is controlled by SDN Controller.
```

- Display local STP status.

```
Qtech(config)#no of stp
Qtech(config)#show of port
STP is controlled by local device.
```

11.5 Monitoring and Maintaining

Clearing Various Information

-

Displaying the Running Status

Command	Function
show of	Displays the status of the current connection between the OpenFlow device and the controller
show of port	Displays the port status of the current OpenFlow device
show of flowtable	Displays the flow table of the current OpenFlow device

Displaying Debugging Information

-