System Basics and Management

QSR-1920, QSR-2920, QSR-3920

Оглавление

1. SYSTEM OPERATION BASICS

1.1. Overview

System operation basics mainly describe the basic knowledge of device operations, including system operation basic functions, device configuration modes, command modes, and command line interface.

1.2. System Operation Basic Functions

Table 1-1 Configuration List of the System Operation Basic Functions

Configuration Task	
Device configuration mode	Device configuration mode
Command operating mode	Command operating mode
Command line interface	Command line interface

1.2.1. Device Configuration Modes

Users can log in to the device for configuration and management in different modes. (For details of the login modes, refer to the chapter "System login" in the configuration guide.) The device provides five typical configuration modes:

- Logging in to the device locally through the Console port. By default, users can configure the device directly in this mode.
- Logging in to the device by remote dial-up through a Modem. The device cannot be configured directly in this mode. That is, before configuration, some preparations need to be made.
- Logging in to the device remotely through Telnet. The device cannot be configured directly in this mode. That is, before configuration, some preparations need to be made.
- Logging in to the device remotely through SSH. By default, the device cannot be configured directly in this mode. That is, before configuration, some preparations need to be made.
- Logging in to the device remotely through web. By default, the device cannot be configured directly in this mode. That is, before configuration, some preparations need to be made.

1.2.2. Command Operating Modes

The device provides a command processing subsystem for management and execution of system commands. The subsystem shell provides the following main functions:

- Registration of system commands
- Editing of system configuration commands by users

- Parsing of the commands that have been inputted by users
- Execution of system commands

If a user configures the device through shell commands, the system provides multiple operating modes for the execution of the commands. Each command mode supports specific configuration commands. In this way, hierarchical protection is provided to the system, protecting the system from unauthorized access.

The shell subsystem provides multiple modes for the operating of configuration commands. These modes have different system prompts, prompting the current system mode of the user. The following lists common configuration modes:

- Common user mode (user EXEC)
- Privileged user mode (privilege EXEC)
- Global configuration mode (global configuration)
- Interface configuration mode (interface configuration)
- File system configuration mode (file system configuration)
- Access list configuration mode (access list configuration)
- Other configuration modes (They will be described in the related sections and chapters.)

The following table shows how to enter the common command modes and switch over between the modes.

Table 1-2 System Modes and Methods of Switching Over Between the Modes

Mode	**How to Enter the Mode**	**System Prompt**	**How to Exit the Mode**	**Functions**
Common user mode	Log in to the device.	`Hostname>`	Run the **exit** command to exit the mode.	Changes the terminal settings. Performs basic tests. Display the system information.
Privileged user mode	In common user mode, run the **enable** command.	`Hostname#`	Run the **disable** or **exit** command to exit to the common user mode.	Configure the operating parameters of the device. Display the operating information of the device.
Global configuration mode	In privileged user mode, run the **configure terminal** command.	`Hostname(config)#`	Run the **exit** command to exit to the privileged user mode.	Configures the global parameters that are required for the device operation.

Interface configuration mode	In global configuration mode, run the **interface** command (while specifying the corresponding interface or interface group).	`Hostname(config-if-xxx[number])#`
		or
		`Hostname(config-if-group[number])#`
			Run the **exit** command to exit to the global configuration mode.
			Run the **end** command to exit to the privileged user mode.
				In this mode, configures device interfaces, including:
				Interfaces of different types
				Interface groups

File system configuration mode	In the privileged user mode, run the **filesystem** command.	`Hostname(config-fs)#`	Run the **exit** command to exit to the privileged user mode.	Manages the file system of the device.

Mode	How to Enter the Mode	System Prompt	How to Exit the Mode	Functions
Access list configuration mode	In global configuration mode, run the **ip access-list standard** or **ip access-list extended** command.	Hostname(config-std-nacl)# Hostname(config-ext-nacl)#	Run the **exit** command to exit to the global configuration mode. Run the **end** command to exit to the privileged user mode.	Configures the Access Control List (ACL). The configuration tasks include: Configuring standard access control lists. Configuring extended access control lists.

Note:

- Hostname is the system name. In global configuration mode, a user can run the hostname command to modify the system name, and the modification takes effect immediately.
- If a user is not in privileged user mode while the user wants to run a privileged mode command, the user can use the do command to run the required command without the need to returning back to the privileged mode. (For details, refer to the related sections in "System Operation Basics" of the command manual.) Note that the mode switchover command such as do configure terminal is not included.

1.2.3. Command Line Interface

The command line interface is a man-machine interface that is provided by the shell subsystem to configure and use the device. Through the command line interface, users can input and edit commands to perform the required configuration tasks, and they can also query the system information and learn the system operation status.

The command line interface provides the following functions for the users:

- System help information management
- System command inputting and editing
- History command management
- Terminal display system management

Command Line Online Help

The command line provides the following types of online help:

- Help
- Full help
- Partial help

Through the above types of online help, users can obtain various help information. The following gives some examples.

- To obtain a brief description of the online help system, input the **help** command in any command mode.

```
Hostname#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 for command 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?'.)
And "Edit key" usage is the following:
   CTRL+A -- go to home of current line
   CTRL+E -- go to end of current line
   CTRL+U -- erase all character from home to current cursor
   CTRL+K -- erase all character from current cursor to end
   CTRL+W -- erase a word on the left of current cursor
   CTRL+R -- erase a word on the right of current cursor
   CTRL+D,DEL -- erase a character on current cursor
   BACKSPACE -- erase a character on the left of current cursor
   CTRL+B,LEFT -- current cursor backward a character
   CTRL+F,RIGHT -- current cursor forward a character
```

- To list all commands and their brief description in any command mode, type "?" in the command mode.

```
Hostname#configure terminal
Hostname(config)# ?
    aaa                Authentication, Authorization and Accounting
    access-list          Access List
    alarm                Set alarm option of system
    apply               Command apply
    arp                Set a static ARP entry
    banner               Define a login banner
    bgp                BGP information
    change               Change user name orpassword
…………………………………………………………………………
```

- Type a command followed by "?", and all sub-commands that can be executed in the current mode are displayed.

```
Hostname#show ?
  access-group         Command access-group
  access-list        List access lists
```

………………………………………………………

- Type a character string followed by "?", and all the key words starting with the character string and their description are displayed.

```
Hostname#show a?
  access-group       Command access-group
  access-list        List access lists
```

………………………………………………………

Command Line Error Messages

For all commands that are typed by users, the command line performs a syntax check. If the commands pass the syntax check, they are executed properly; otherwise, the system reports error messages to the users. The following table shows common error messages.

Table 1–3 Command Line Error Messages

Error Message	Error Cause
% Invalid input detected at '^' marker.	No command or key word is found, the parameter type is incorrect, or the parameter value is not within the valid range.
Type "*** ?" for a list of subcommands or % Incomplete command	The inputted command is incomplete.
Hostname#wh % Ambiguous command: wh % Please select: whoami who	The inputted character string is a fuzzy command.

History Commands

The command line interface provides a function that is similar to the Doskey function. The system automatically saves the user inputted commands into the history command cache. Then, users can invoke the history commands saved by the command line interface at any time and execute the command repeatedly, reducing unnecessary efforts in re-typing the commands. The command line interface saves up to 20 commands for each user that is connected to the device. Then, new commands overwrite old ones.

Table 1-4 Accessing History Commands of the Command Line Interface

To...	Press...	Execution Result
Access the previous history command	The up arrow key ↑ or Ctrl+P keys	If an earlier history command is available, it is displayed. If no earlier history command is available, an alarm sound is played.
Access the next history command	The down arrow key ↓ or Ctrl+P keys	If a later history command is available, it is displayed. If no later command is available, the commands are cleared, and an alarm sound is played.

Note:

- If you want to access history commands by using the up and down arrow keys, when you telnet to the device in the Windows 98 or Windows NT OS, set Terminals > Preferred Options > Simulation Options to VT-100/ANSI.
- History command display is based on the current command mode. For example, if you are in privileged mode, only history commands in privileged mode are displayed.

Editing Features

The command line interface provides basic command editing functions. It supports multi-line editing. Each line of command can contain up to 256 characters. The following table lists the basic editing functions that are provided by the shell subsystem for the command line interface.

Table 1-5 Basic Editing Functions

Key	Function
A common key	If the edit buffer is not full, the character is inserted to the position of the cursor, and the cursor moves to the right. If the edit buffer is full, an alarm sound is played.
The Backspace key	Deletes the character before the cursor and moves the cursor backward. If the cursor reaches the beginning of the command, an alarm sound is played.
The Delete or Ctrl+D key	Deletes the character behind the cursor. If the cursor reaches the end of the command, an alarm sound is played.

Key	Function
The left arrow key ← or Ctrl+B keys	Moves the cursor one characters to the left. If the cursor reaches the beginning of the command, an alarm sound is played.
The right arrow key → or Ctrl+F keys	Moves the cursor one characters to the right. If the cursor reaches the end of the command, an alarm sound is played.
The up and down arrow keys ↑↓	Display history commands.
Ctrl+A	Moves the cursor to the beginning of the command line.
Ctrl+E	Moves the cursor to the end of the command line.
Ctrl+K	Delete all characters at the right of the cursor until the end of the command line
Ctrl+R	Delete a word at the right of the cursor
Ctrl+U	Deletes all characters on the left of the cursor till the beginning of the command line.
Ctrl+W	Delete a word at the left of the cursor

Display Features

To facilitate users, the command line interface provides the following display features:

If the information to be displayed is more than one screen, the pause function is provided, and the prompt "---MORE---" is displayed at the lower left corner of the screen. At this time, the options displayed in the following table are available for users.

Table 1-6 Display Features

Key	Function
Space key, down arrow key ↓, or Ctrl-F	Display the next screen.
The up arrow key ↑ or Ctrl-B keys	Display the previous screen.
The Enter key, right arrow key → or equal key =	Scroll the displayed information one line down.
The left arrow key ← or the minus key -	Scroll the displayed information one line up.
Ctrl-H	Returns back to the topmost part of the displayed information.
Any other keys	Exits the display. Then, the information that has not been displayed will not be displayed.

2. SYSTEM LOGIN

2.1. Overview

The device supports the following system login modes:

- Logging into the device through the Console port for management and maintenance.
- Logging into the device through the AUX port for management and maintenance.
- Telnet (remote login). Users can manage and maintain the device remotely in this mode.
- Secure Shell (SSH). Through its encryption and authentication technology, SSH provides secure remote login management services for users.
- Telnet (remote login). Users can manage and maintain the device remotely in this mode.

2.2. System Login Function Configuration

Table 2-1 System Login Function Configuration List

Configuration Tasks	
Logging in to the device through the Console port	-
Logging in to the device through the AUX port	-
Configuring remote login through Telnet	Enable the Telnet service of the device.
	The device acts as a Telnet client for remote login.
Configuring remote login through SSH	Enable the SSH service of the device.
	The device acts as an SSH client for remote login.
Configuring remote login through web	Configure logging into the device via HTTP
	Configure logging into the device via HTTPS

Note:

- For the related user configuration of Telnet, SSH, and web remote login, refer to the LUM chapter.

2.2.1. Log in to Device via Console Port

To connect a terminal to the device through the Console port to configure the device, perform the following steps:

Step 1: Select a terminal.

The terminal can be a terminal with a standard RS-232 serial port or an ordinary PC, and the latter one is more frequently used. If the remote dial-up login mode is selected, two Modems are required.

Step 2: Connect the physical connection of the Console port.

Ensure that the terminal or the device that provides the Console port has been powered off, and then connect the RS-232 serial port of the terminal to the Console port of the device. The following figure shows the connection.

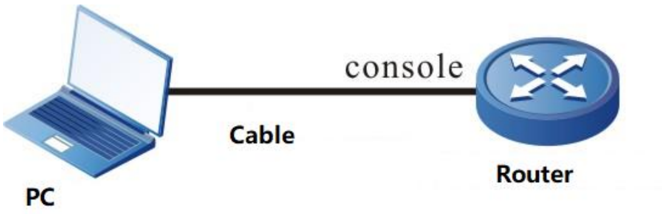


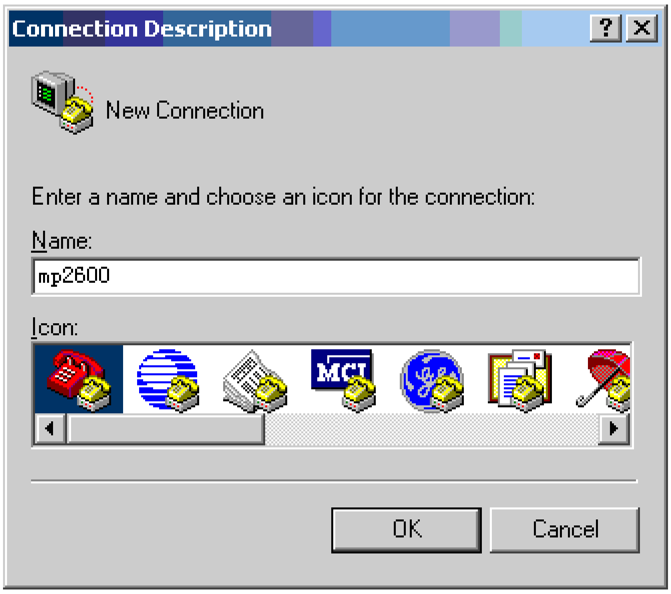
Figure 2-1Connection for Login via the Console Port

Step 3: Configure the HyperTerminal.

After powering on the terminal, you need to set the communication parameters of the terminal, that is, baud rate of 9600 bps, 8 data bits, 1 stop bit, no parity check, and no data stream control. For a PC with the Windows XP or Windows NT OS, run the HyperTerminal program, and set the communication parameters of the serial port of the HyperTerminal according to the previously mentioned settings. The following takes the HyperTerminal in the Windows NT OS for example.

- Create a connection:

Input a connection name, and select a Windows icon for the connection.



New Connection

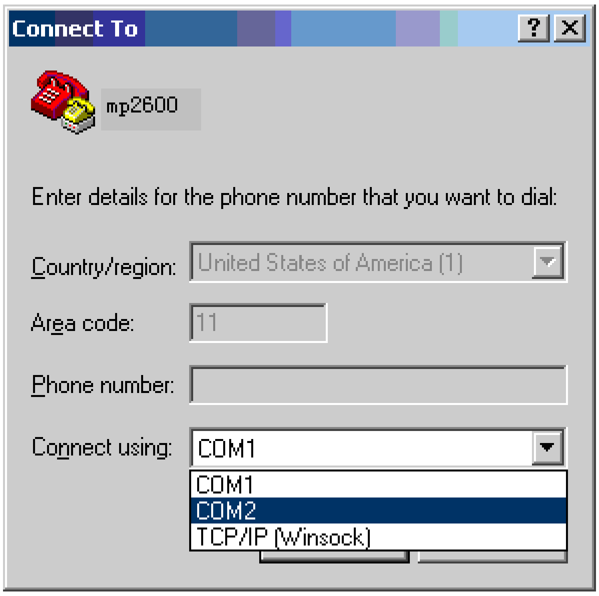
Enter a name and choose an icon for the connection:

Name: mp2600

Figure 2-2 Creating a Connection

- Select a serial communication port:

According to the serial communication port that has been connected, select COM1 or COM2.



mp2600

Enter details for the phone number that you want to dial:

Country/region: United States of America (1)

Area code: 11

Phone number:

Connect using: COM1

COM1
COM2
TCP/IP (Winsock)

Figure 2-3 Selecting a Serial Communication Port

- Configure parameters for the serial communication port:

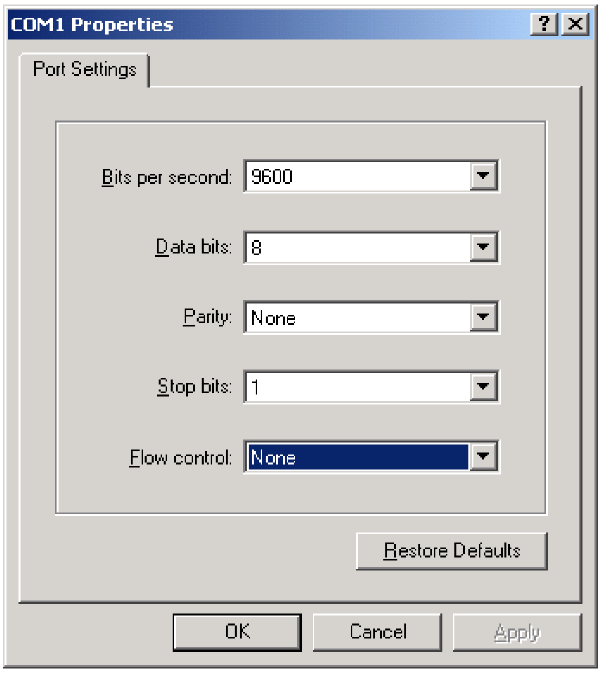
Baud rate: 9600 bps

Data bit: 8 bits

Parity check: None

Stop bit: 1 bit

Data stream control: None



Bits per second: 9600

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

Figure 2-4 Configuring Parameters for the Serial Communication Port

- Login success authentication:

After the device with the Console port is powered on, the startup information of the device is displayed on the terminal. After the startup is completed, the "Press any key to start the shell!" message is displayed. If login authentication is configured to be required, input the user name and password; otherwise, press any key to log in directly. After the login succeeds, the "Hostname>" prompt is displayed on the terminal. Then, you can configure the device.

2.2.2. Log into Device via AUX Port

Because the Console port on the device has the function of the AUX port, the device login can be realized through external modem remote dial-up connection. When using aux port for remote dial-up login, two modem devices are needed, and pre configuration is needed before configuring the function of connecting the AUX port to Modem, that is, entering terminal mode in configuration mode and configuring automatic detection Modem. The command configuration is as follows:

```
Hostname # configure terminal
Hostname (config)#line con 0
Hostname (config-line)#modem auto-detection
```

We will introduce how to log into the device through the AUX port from the following aspects:

Application Mode of Logging into Device via Remote Dialing

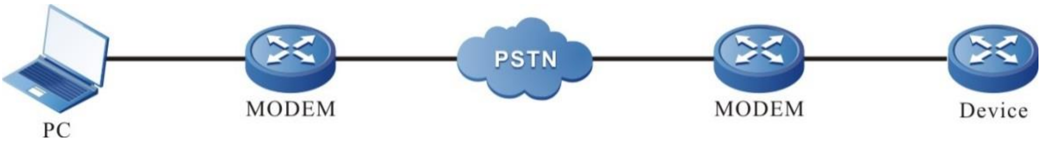


Figure 2-2 Application mode of logging into the device via remote dialing

Description of physical connection via remote dialing:

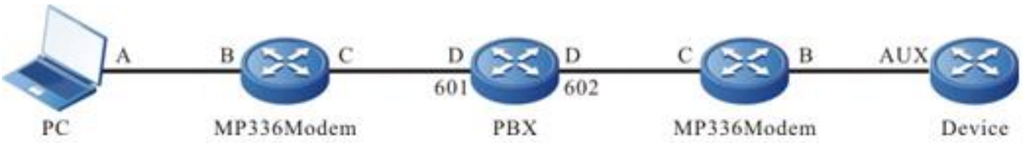


Figure 2-3 Description of physical connection via remote dialing:

Interface A—PC serial port.
Interface B—MP336 Modem DB25 port, "DB25 pin to RJ45 hole adapter" is required.
Interface C—MP336 Modem “Dial” cable interface
Interface D—PBX internal interface, as shown in the figure, the two modems are respectively connected to the 601 and 602 ports of PBX.
Cable a—The general console port configuration line of our products;
Cable b—Ordinary telephone line;
Cable c—AUX dedicated line.

Description of Connection Method via Remote Dialing

Taking the MP336 band Modem as an example, we will describe how to dial from PC to the Console port of the device through the Modem.

Step 1: Dial the dialing switch after MP336 Modem to “0001”.

Step 2: Connect the Console cable connected to the PC to the “DB25 pin to RJ45 hole” adapter on MP336 Modem.

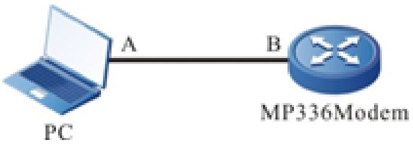


Figure 2-4 Description of connection method through remote dialing

Step 3: Open the corresponding COM port with SecureCRT or HyperTerminal.

Step 4: Turn on the power of MP336 Modem. After hearing "diddidi", input "cdmp" continuously, and you can see the configuration interface of MP336 Modem.

Step 5: Set both MP336 Modems to the following mode (the following figure shows only the settings of the responder).

Step 6: Setting Modem is completed.

Use the Dial-up Function of HyperTerminal to Connect

Step 1: Connect according to the above application mode of remote dial-up login device, and turn on the power of each device.

Step 2: Take the PC of Windows XP system as an example, you will be prompted:

Step 3: After the driver is installed automatically, the system will display the following:

Step 4: If installing successfully, you can see the newly installed modem in the device manager, as shown in the following figure:

Open HyperTerminal to Create One Connection

Open the HyperTerminal and create a new connection. When selecting connection, use Rockwell 5600External Modem If the above driver installation fails, there is no such option.)

2.2.3. Configure Remote Login via Telnet

Configuration Condition

None

Enable Telnet service of Device

A user can log in to the device remotely through Telnet for management and maintenance. Before using the Telnet service, enable the Telnet service of the device. After the Telnet service of the device is enabled, the Telnet service port 23 is monitored.

Table 2-2 Enabling the Telnet Service of the Device

Step	**Command**	**Description**
Enter the global configuration mode.	**configure terminal**	-
Enable the Telnet service of the device.	**telnet server enable**	Mandatory. By default, the Telnet service is enabled.

Take Device as Telnet Client for Remote Login

The user takes the device as a Telnet client to log in to the specified Telnet server for configuration and management.

Table 2-3 Taking the Device as a Telnet Client for Remote Login

Step	**Command**	**Description**
Enter the global configuration mode.	**configure terminal**	-
Enable the Telnet client of the device.	**telnet client enable**	Optional. By default, the Telnet client is enabled.
Take the device as a Telnet client for remote login.	**telnet** [**vrf** *vrf-name*] { *hostname* | *remote-host* } [*port-number*] [**ipv4** | **ipv6**] [**source-interface** *interface-name*]	Mandatory.

Note:

- The Telnet client can log in to a remote device only when the Telnet server function of the remote device is enabled, and the network between the Telnet client and the remote device is normal.

2.2.4. Configure Remote Login via SSH

Configuration Condition

None

Enable the SSH Service of the Device

After the SSH server of a device is enabled, the device accepts the connection request initiated by the user from the SSHv1 or SSHv2 client. After the client passes the authentication, the client can access the device. After the SSH service of the device is enabled, the SSH service port 22 is monitored. If the **ip ssh server** or **ipv6 ssh server** command is configured without parameter **sshv1-compatible**, it indicates that an SSH client can log in only through SSHv2.

Table 2-4 Enabling the SSH Service of the Device

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the IPv4 SSH service of the device.	**ip ssh server** [**sshv1-compatible**] [listen-port]	Mandatory. By default, the IPv4 SSH service is disabled.
Enable the IPv6 SSH service of the device	**ipv6 ssh server** [**sshv1-compatible**] [listen-port]	Mandatory By default, the IPv6 SSH service is disabled.

As SSH Server, Device Support Selecting Protocol Algorithm

As a server, the device supports selecting data compression algorithm, public key algorithm, secret key exchange algorithm, encryption algorithm and HMAC (hashed message authentication code) algorithm in SSH protocol. The above algorithms are configured with ssh server as the starting command, followed by the corresponding commands of **prefer-compress**, **prefer-identity-key**, **prefer-key**, **prefer-stoc-cipher**, **prefer-stoc-hmac**. By default, the above protocol algorithms support all optional algorithms.

Table 2-5 Configure SSH server protocol algorithm

Step	**Command**	**Description**
Enter the global configuration mode.	**configure terminal**	-
Configure the SSH server compression algorithm	**ssh server prefer-compress** [none | zlib | zlib-openssh]	Optional By default, three algorithms are supported.
Configure SSH server public key algorithm	**ssh server prefer-identity-key** [ssh-dss | ssh-rsa]	Optional By default, two algorithms are supported.
Configure ssh server secret key exchange algorithm	**ssh server prefer-key** [diffie-hellman-group-exchange-sha256 | diffie-hellman-group-exchange-sha1 | diffie-hellman-group14-sha1 | diffie-hellman-group1-sha1]	Optional By default, four algorithms are supported.
Configure SSH server encryption algorithm	**ssh server prefer-stoc-cipher** [aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc | 3des-cbc | cast128-cbc | arcfour | aes192-cbc | aes256-cbc | blowfish-cbc | arcfour128 | arcfour256 | rijndael-cbc-lysator | sm4-cbc]	Optional By default, fourteen algorithms are supported.
Configure the HMAC algorithm of the SSH server	**ssh server prefer-stoc-hmac** [hmac-md5 | hmac-sha1 | umac-64-openssh | hmac-ripemd160 | hmac-ripemd160-openssh | hmac-sha1-96 | hmac-md5-96]	Optional By default, seven algorithms are supported.
Configure SSH server dual-factor authentication	**ssh authentication-type password-publickey**	Optional By default, dual-factor authentication function is disabled.

Note:

- The data encryption algorithm supported by the device as ssh server is not only affected by the configuration of ssh server prefer-stoc-cipher, but also limited by the configuration of the security mode (ssac mode). That is to say, the data encryption algorithm actually supported by the device as ssh server must meet the above two configurations at the same time.

- The public key algorithm specified by the device as the ssh server is not only affected by the configuration of prefer-identity-key, but also limited by the configuration of SSH public key length (ssh hostKey length). When the length of SSH public key is 2048, the device only supports the ssh-rsa algorithm as ssh server.

Configure Device SSH Key Re-negotiation Function

The device supports specifying the life cycle of the SSH key renegotiation in time, and also the traffic cycle of the SSH key negotiation in traffic.

Table 2-6 Configure the SSH key re-negotiation function of the device

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the specified time-based SSH key renegotiation life cycle	**ssh re-exchange** [**minutes** *minutes-number*]	Mandatory By default, time-based SSH key re negotiation is not enabled
Configure the traffic period of SSH key renegotiation measured by traffic	**ssh re-exchange** [**kbytes** *kbytes-number*]	Mandatory By default, SSH key renegotiation measured by traffic is not enabled

Take the Device as an SSH Client for Remote Login

The device acts as an SSH client to log in to the specified SSH server remotely through the SSHv1 or SSHv2 protocol. During the login, a user name and a password are required for authentication from the SSH server.

Table 2-7 Taking an SSH Client for Remote Login

Step	Command	Description
Take the device as an SSH client for remote login.	**ssh** [**vrf** *vrf-name*] **version** { **1 | 2** } *remote-host port-number*[**source-interface** *interface-name* **]** *user* **auth-method 1** *password*	Mandatory.

Note:

- The SSH client can log in to a remote device only when the SSH service of the remote device is enabled, and the network between the SSH client and the remote device is normal.

Take the Device as an SFTP Client to Access SFTP Server

The device acts as an SFTP client to log in to the specified SFTP server remotely through the SSHv2 protocol. During the login, a user name and a password are required for authentication from the SFTP server. After the SFTP client is connected to the SFTP server, download or upload the files on the server.

Table 2-8 Taking the Device as SFTP Client to Access the SFTP Server

Step	Command	Description
Take the device as the SFTP client to access the SFTP server.	**sftp {get | put}** [**vrf** *vrf-name*] *remote-host port-number* [**source-interface** *interface-name*] *user password src-filename dst-filename* **[compress]**	Mandatory

Note:

- The SFTP client can log in to a remote device only when the SSH service of the remote device is enabled, and the network between the SFTP client and the remote device is normal.

2.2.5. Configure Remote Login via WEB

In order to facilitate the configuration and maintenance of network equipment, the device provides Web network management function. The device provides a built-in web server. You can log in to the device through a browser on PC, and configure and maintain the device intuitively by using the web interface. The device supports two built-in web login modes: http login mode and HTTPS login mode. The device supports IPv4 web login and IPv6 web login.

Configuration Conditions

No

Configure Logging into Device via HTTP

Users can log into the device remotely through HTTP for related management and maintenance. However, before logging into the device through HTTP, you need to enable the HTTP service of the device first.

Table 2-9 Configure logging into the device via HTTP

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-

Step	Command	Description
Enable the HTTP server	**ip http server**	Mandatory By default, do not enable the web server.
Configure the port of the HTTP server	**ip http port** *port_number*	Optional By default, the port number of the HTTP server is 80.

Note:

- Before starting the HTTP server, you must copy the corresponding WEB ROM file to /flash.

Configure Logging into Device via HTTPS

Users can remotely log into the device through the HTTPS mode for related management and maintenance, but before logging into the device through the HTTPS mode, they need to start the HTTPS service of the device.

Table 2-10 Configure logging into the device via HTTPS

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the HTTP server	**ip http server**	Mandatory By default, do not enable the WEB server.
Enable the HTTPS server	**ip http secure-server**	Mandatory By default, do not enable the WEB server.
Configure the port of the HTTPS server	**ip http port** *port_number*	Optional By default, the port number of the HTTPS server is 443.
Configure the certificate used by the HTTPS service	**ip http certificate** *ca-store*	Optional By default, the HTTPS service uses the self-signed certificate.

Note:

- For the configuration of the trust domain and the import of the certificate, please refer to the relevant sections of PKI.

2.2.6. System Login Monitoring and Maintaining

Table 2-11 System Login Monitoring and Maintaining

Command	Description
show fingerprint	Display the fingerprint information of the SSH public key.

2.3. Typical Configuration Example of System Login

2.3.1. Configure a Local Terminal to Telnet to the Device

Network Requirements

- A PC is used as a local terminal to log in to the device through Telnet.
- A route must be available between the PC and the device.

Network Topology

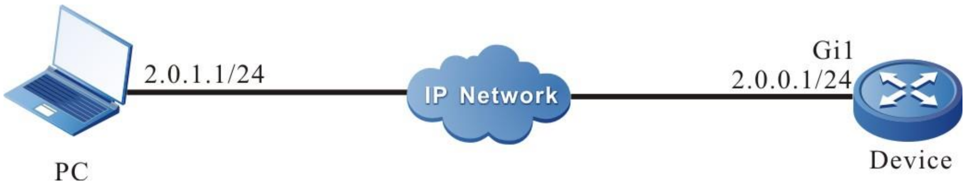


Figure 2-5 Network Topology for Configuring a Local Terminal to Telnet to the Device

Configuration Steps

Step 1: Configures IP address for gigaethernet1. (Omitted)

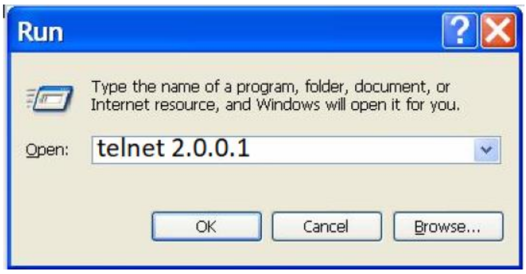
```
Device>enable
Device#configure termin
Device(config)#interface gigaethernet1
Device(config-if-gigabitethernet1)#ip address 2.0.0.1 255.255.255.0
```

Step 2: Configure the **enable** password.

```
Device>enable
Device#configure terminal
Device(config)#enable password admin
```

Step 3: Telnet to the device.

#On the PC, run the Telnet program, and input the IP address of gigaethernet1, as shown in Figure 2-9.

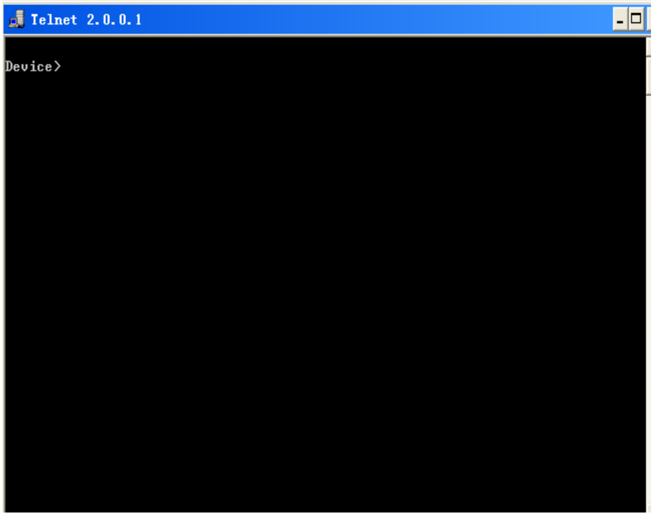

Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
OK
Cancel
Browse...

telnet 2.0.0.1

Figure 2-6 Telnet to the device on the PC

Step 4: Check the result.

#If the login succeeds, a window as shown in the following figure is displayed.



```
Device>
```

Figure 2-7 Window Displayed after Telnet Success

After logging in to the device successfully, input the correct **enable** password to obtain the required operation rights of the device. To log out of the device, input the **exit** command continuously or use the shortcut key "Ctrl + C" to exit directly.

Note:

- If the "Too many clients or invalid access" message is displayed, it indicates that the number of login users has reached the maximum allowed number of login users of the device. In this case, wait a while and try to log in again.
- If the "%login operation is locked by login-secure service" message is displayed, it indicates that the times of user name password input errors exceeds the times of continuous login authentication failures. If reaching the times specified by the system, the system rejects the login connection request from the IP address during the specified time.
- If the "Password required, but none set" message is displayed, it indicates that no login password has been configured.

2.3.2. Configure the Local Device to Log into a Remote Device via Telnet

Network Requirements

- The local device Device1 acts as the Telnet client, while the remote device Device2 acts as the Telnet server.
- A route must be available between the two devices.

- The PC can normally log in to Device1.

Network Topology

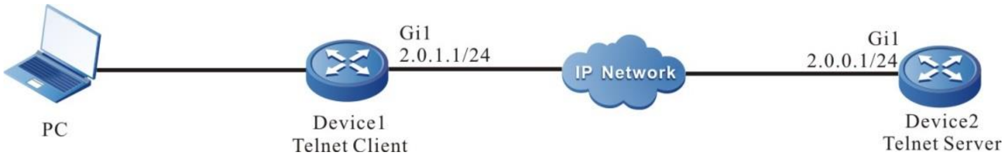


Figure 2-8 Network Topology for Configuring a Local Device to Telnet to a Remote Device

Configuration Steps

Step 1: Use PC to log into Device1. (omitted)

Step 2: Configure the IP address and the enable password of Device2. (Omitted)

Step 3: On Device1, run the following command to Telnet to Device2.

```
Device1>enable
Device1#telnet 2.0.0.1
```

#Enter the shell screen of Device2.

```
Connect to 2.0.0.1 ...done
Device2>
```

After logging in to the Device2 successfully, input the correct enable password to obtain the required operation rights of the device. To log off the device, input the **exit** command continuously, or use the shortcut key “ctrl+c” to exit directly.

2.3.3. Configure the Local Device to Log into a Remote Device via SSH

Network Requirements

- The local device Device1 acts as the SSH client, while the remote device Device2 acts as the SSH server.
- A route must be available between the two devices.
- The PC can normally log in to Device1.

Network Topology

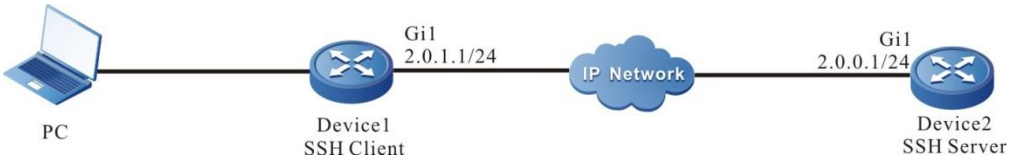


Figure 2-9 Network Topology for Configuring a Local Device to Log in to a Remote Device via SSH

Configuration Steps

Step 1: Configure a local user and the related properties.

#Configure Device2.

```
Device2#configure terminal
Device2(config)#local-user admin1 class manager
```

```
Device2(config-user-manager-admin1)#service-type ssh
Device2(config-user-manager-admin1)#password 0 admin1
Device2(config-user-manager-admin1)#exit
```

Step 2: Enable the SSH server function of Device2.

```
Device2(config)#ip ssh server
```

Step 3: Set the login authentication mode to local authentication, letting the device login adopt the local authentication.

- Device2(config)#line vty 0 15
- Device2(config-line)#login aaa

Step 4: #On Device1, log in to Device2 through SSH.

#Configure Device1.

```
Device1#ssh  version  2 2.0.0.1  22 admin1 auth-method 1 admin
The authenticity of host '2.0.0.1' can't be established
DNS SPOOFING is happening or the IP address for the host and its host key have changed
RSA key fingerprint is 7b:ed:cc:81:cf:12:36:6f:f7:ff:29:15:63:75:64:10.
Are you sure you want to continue connecting (yes/no)? yes
```

Step 5: Check the result.

If the login succeeds, the shell screen of Device2 is displayed.

2.3.4. Configure the Local Device to Log into a Remote Device via IPv6 SSH

Network Requirements

- The local device Device1 acts as the IPv6 SSH client, while the remote device Device2 acts as the IPv6 SSH server.
- A route must be available between the two devices.
- The PC can normally log in to Device1.

Network Topology

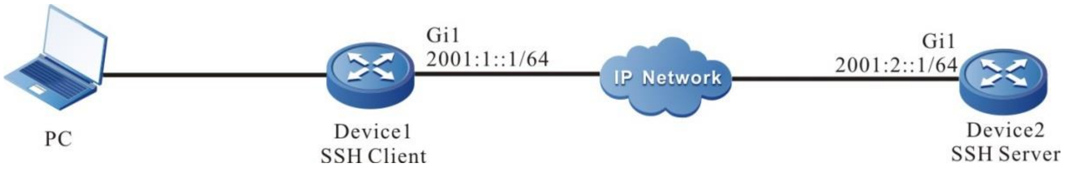


Figure 2-10 Configure logging into the remote device via IPv6 SSH of the local device

Configuration Steps

Step 1: Configure the local user and the related attributes.

# Configure Device2.

```
Device2>enable
Device2#configure terminal
```

```
Device2(config)#local-user admin1 class manger
Device2(config-user-manager-admin1)#password 0 admin
Device2(config-user-manager-admin1)#service-type ssh
Device2(config-user-manager-admin1)#exit
```

Step 2: Enable the IPv6 SSH server function of Device2.

```
Device2(config)#ipv6 ssh server
```

Step 3: Configure the login authentication mode to use the local authentication.

```
Device2(config)#line vty 0 15
Device2(config-line)#login aaa
```

Step 4: Log into Device2 via IPv6 SSH on Device1.

# Configure Device1.

```
Device1#ssh  version  2 2001:2::1  22 admin1 auth-method 1 admin
The authenticity of host '2001:2::1' can't be established
DNS SPOOFING is happening or the IP address for the host and its host key have changed
RSA key fingerprint is 7b:ed:cc:81:cf:12:36:6f:f7:ff:29:15:63:75:64:10.
Are you sure you want to continue connecting (yes/no)? yes
```

Step 5: Check the result.

After logging in successfully, enter the shell interface of Device2.

2.3.5. Configure the Local Device to Log into a Remote Device via WEB

Network Requirements

- Use PC as local terminal to log into the device through web.
- The route between the two devices must be reachable.

Network Topology

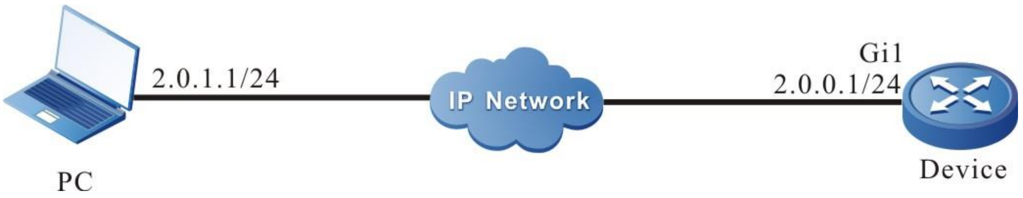


Figure 2-11 Configure the local device to log into the remote device via web

Configuration Steps

Step 1: Configure the related attributes of the local user.

#Configure Device.

```
Device>enable
```

```
Device#configure terminal
Device(config)#local-user admin1 class manger
Device(config-user-manager-admin1)#password 0 admin
Device(config-user-manager-admin1)#service-type web
Device(config-user-manager-admin1)#privilege 15
Device(config-user-manager-admin1)#exit
```

#Configure local authorization to make the local user authorization attribute take effect

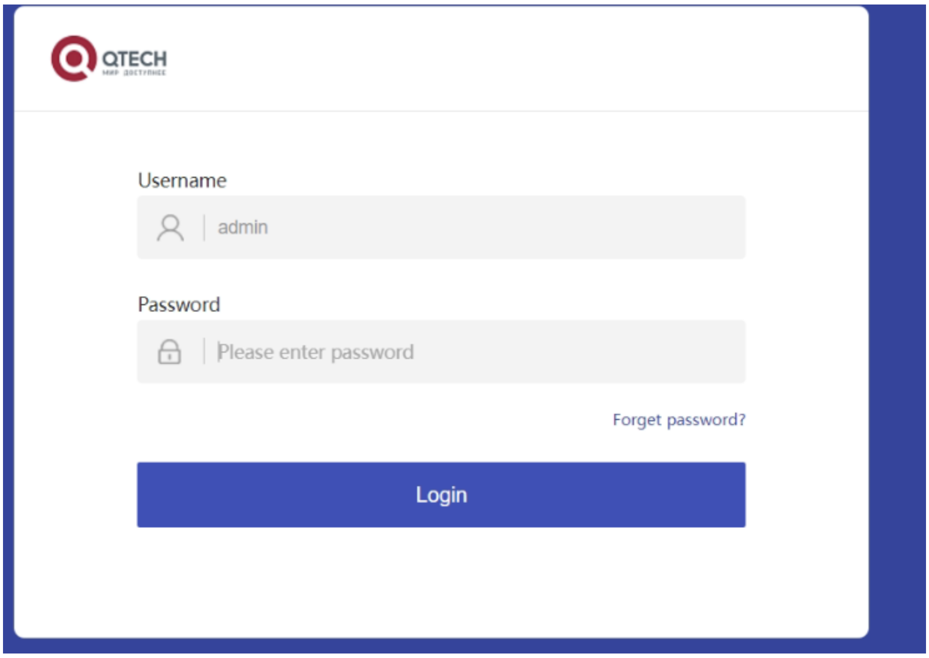
```
Device(config)#domain system
Device(config-isp-system)#aaa authorization login local
Device(config-isp-system)#exit
```

Step 2: Enable the https service.

```
Device#configure terminal
Device(config)#ip http server
Device(config)#ip http secure-server
Are you sure open https (Yes|No)?y
 The HTTP secure-server open, WEB Server will be automatically restart.
```

Step 3: Use the device IP address to log into the device via the browser.

# Enter the configured local administrator user name and password.



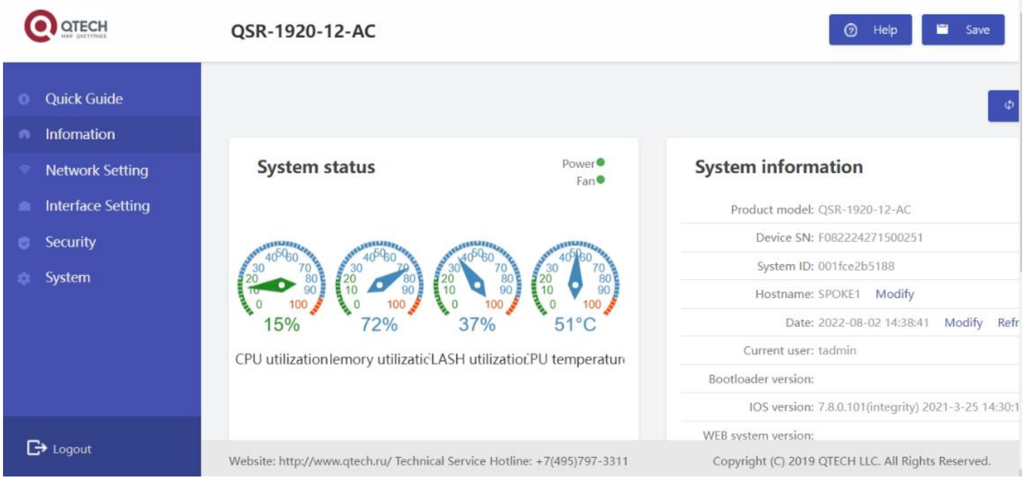
Username: admin

Password: Please enter password

Figure 2-12 Input the user name and password of the device

Step 4: Check the result.

#Enter the web interface after logging in successfully.



System status

Power ●
Fan ●

15% CPU utilization

72% Memory utilization

37% FLASH utilization

51°C CPU temperature

System information

Product model: QSR-1920-12-AC

Device SN: F082224271500251

System ID: 001fce2b5188

Hostname: SPOKE1 Modify

Date: 2022-08-02 14:38:41 Modify Refr

Current user: tadmin

Bootloader version:

IOS version: 7.8.0.101(integrity) 2021-3-25 14:30:1

WEB system version:

Website: http://www.qtech.ru/ Technical Service Hotline: +7(495)797-3311

Copyright (C) 2019 QTECH LLC. All Rights Reserved.

Figure 2-13 Successful login interface

3. SYSTEM CONTROL AND MANAGEMENT

3.1. Overview

To enhance the operation security of the device, in user login or enable operation, the device provides multiple authentication management types (including AAA. Refer to the related sections and chapters in AAA configuration manual.) Only the user with the required operation rights can log in or perform the **enable** operation successfully.

To authorize different set of executable commands to different level of users, the device commands are divided into levels 0-15, and user levels are divided into levels 0-15. Among the levels, level 0 has the lowest rights while level 15 has the highest rights.

3.2. Login Control and Management Function Configuration

Table 3-1 Configuration List of Login Control and Management

Configuration Tasks	
Switch over between user levels.	Switch over between user levels.
Configure the command level.	Configure the command level.
Configure the **enable** password.	Configure the **enable** password.
Configure line properties.	Enter the line configuration mode of the Console port.
	Enter the line configuration mode of the Telnet or SSH user.
	Configure the absolute time for the login user operation.
	Configure the privilege level of the login user.
	Configure users to automatically execute commands after login.
	Configure auto command execution options.

Configuration Tasks	
	Configure login user idle timeout time.
	Configure the line password.
	Configure the line using attributes.
	Configure the login authentication mode.
	Enable the Modem function of the Console port.
	Configure the user login timeout time.

3.2.1. Switch Over Between User Levels

If a user name and password of the corresponding level is configured, the user can run the **enable level (0-15)** command and then enter the correct password to enter the required user level. Meanwhile, the user has the execute permission of the user level and the lower levels.

- If the current user level is higher than the user level that the user wants to enter, then no authentication is required, and the user directly enters the required user level. If the user level that the user wants to enter is higher than the current user level, authentication is required according to the current configuration, and the authentication mode is selected according to the configuration.
- If the **enable** password of the corresponding level has been configured (by using the **enable password level** command), while the enable authentication of Authorization, Authentication and Accounting (AAA) is not configured or the AAA enable authentication is set to use the enable method, use the **enable** password for authentication.
- If the **enable** password of the required level has not been configured, but the enable authentication method is set to use the local enable password for authentication, there are two cases:

a) In the case of a Telnet user, the login fails. If AAA has not been configured, the "% No password set" is prompted. If AAA has been configured, the "% Error in authentication" message is prompted.

b) For a Console port user, try to use the enable password for authentication during the login. If the enable password has not been configured, use the none authentication method. That is, the login passes the authentication by default.

If enable authentication succeeds, the user enters the specified user level and the user has execution permission of the level. To query the user level of the current user, run the **show privilege** command.

If the **aaa authentication enable method** is configured and a related method is used to enable authentication, then the related method is required for authentication, including:

a) If aaa authentication enable method none is configured, no password is required.

b) If aaa authentication enable-method radius-group is configured, Remote Authentication Dial in User Service (RADIUS) authentication is used. Note that the enable authentication user names for RADIUS are fixed, that is, $enab+level$. Here "level" is a number in the range of 1-15, that is, the level that the user wants to enter. The RADIUS user names are fixed, therefore, during authentication, no user name is required. The user needs only to input the password. If passwords have been set for users of different levels on the RADIUS server, after inputting the correct password, the login succeeds; otherwise, the login fails. For example, in running the enable 10 command, the fixed user name is $enab10$. If the user name exists on the RADIUS server, input the password corresponding to the user name, and then the authentication succeeds.

c) If aaa authentication enable-method tacacs-group is configured, Terminal Access Controller Access Control System (TACACS) authentication is used. If the user name is displayed during login, keep the user name for login, and input the enable password of the user name. Otherwise, input a user name and the enable password of the user name. If the inputted user name exists in the TACACS server and the enable password of the TACACS has been set, the authentication succeeds; otherwise, the authentication fails.

Note:

- The previously mentioned enable authentication methods can form a combination in use.

Configuration Condition

None

Switch Over Between User Levels

If a user has the corresponding authority, the user can switch from the common user mode to the privileged user mode by switching over between user levels with a command. Then, the user has the authority of the user level. If a user runs the command in the privileged user mode, the user level switchover is performed according to the command parameter.

Table 3-2 Switching over between User Levels

Step	Command	Description
Switch over between user levels.	**enable** [*level-number*]	Mandatory. By default, the user level is level 15.

3.2.2. Configure the Command Level

Configuration Condition

None

Configure the Command Level

In the application program, each shell command has a default level, which can be modified through the **privilege** command. A user can execute only the commands with the level equal to or smaller than the user level. For example, a user with the user level 12 can execute only the commands with the levels 0-12. In configuring the command level, you need to make use of command modes. You can modify the level of a single command or all commands in a specified command mode.

Table 3-3 Configuring the Command Level

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the command level.	**privilege** *privilege-mode* **level** *level-number* [**all | command** *command-line*]	Mandatory.

3.2.3. Configure the enable Password

Configuration Condition

None

Configure the enable Password

The enable password is the password that is used by a level of users to enter the local level. If no level is specified in the enable command, the password is set as the enable password of level 15 by default.

Table 3-4 Configuring the enable password

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the **enable** password.	**enable password** [**level** *level-number*] [**0**] *password*	Mandatory. By default, no enable password is configured.

3.2.4. Configure Line Properties

The device supports up to one Console port user and 16 Telnet or SSH users to log in at the same time. Line commands can set different authentication and authorization properties for the login users.

Configuration Condition

None

Enter Line Configuration Mode of Console Port

To configure the Console port properties, you need to enter the line configuration mode of the Console port.

Table 3-5 Entering the Line Configuration Mode of the Console Port

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enters the line configuration mode of the Console port.	**line con 0**	Mandatory

Enter the Line Configuration Mode of the Telnet or SSH User

To configure the Telnet or SSH properties, you need to enter the line configuration mode of Telnet of SSH.

Table 3-6 Entering the Line Configuration Mode of the Telnet or SSH User

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the line configuration mode of the Telnet or SSH user.	**line vty** { *vty-min-number* } [*vty-max-number*]	Mandatory

Configure Absolute Time for Login User Operation

The absolute time for the login user operation refer to the timeout time from the successful login of a user to the automatic exit of the user, in the unit of minute. If the absolute time is set to 0, it indicates that the time is not limited. By default, the time is 0. In addition, five seconds before the configured time expires, the following prompt message is displayed: Line timeout expired.

Table 3-7 Configuring the Absolute Time for the Login User Operation

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the line configuration mode of the Console port or Virtual Type Terminal (VTY).	**line** { **con 0** | **vty** *vty-min-number* [*vty-max-number*] }	Mandatory

Step	Command	Description
Configure the absolute time for the login user operation.	**absolute-timeout** *absolute-timeout-number*	Mandatory. By default, the absolute time is 0, that is, no time limit.

Configure Privilege Level of Login User

Configure the privilege level of the login user. The default privilege level is 1. A user can execute only the commands with the level equal to or smaller than the current level.

Table 3-8 Configuring the Privilege Level of the Login User

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the line configuration mode of the Console port or VTY.	**line** { **con 0** | **vty** *vty-min-number* [*vty-max-number*] }	Mandatory.
Configure the privilege level of the login user.	**privilege level** *level-number*	Mandatory. The privilege level is 1.

Configure Users to Automatically Execute Commands after Login

Configure the commands to be automatically executed after users successfully log in. By default, no command is to be automatically executed.

Table 3-9 Configuring the Commands to be Automatically Executed after Successful Login

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the line configuration mode of the Console port or VTY.	**line** { **con 0** | **vty** *vty-min-number* [*vty-max-number*] }	Mandatory
Configure the commands to be automatically executed after successful login.	**autocommand** *command-line*	Mandatory

Configure Auto Command Execution Options

You can configure delay time for auto commands, and configure whether to disconnect the user connection after the commands are executed automatically. By default, the command execution is not delayed, and the user connection is disconnected after the commands are executed automatically.

The auto command execution options include delay and whether to disconnect the user connection after command execution.

Table 3-10 Configuring Auto Command Execution Options

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the line configuration mode of the Console port or VTY.	**line** { **con 0** | **vty** *vty-min-number* [*vty-max-number*] }	Mandatory.
Configure the auto command execution options.	**autocommand-option** { **nohangup** [**delay** *delay-time-number*] | **delay** *delay-time-number* [**nohangup**] }	Mandatory.

Note:

- The **autocommand-option** command is valid only after the autocommand function is configured.

Configure Login User Idle Timeout Time

If the time in which login user does not perform any operation on the device is longer than the idle timeout time, the device make the current login user to log out. The default idle timeout exit time is 5 minutes. If the time is set to 0, then idle timeout does not take effect.

Table 3-11 Configuring the Idle Timeout Exit Time

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the line configuration mode of the Console port or VTY.	**line** { **con 0** | **vty** *vty-min-number* [*vty-max-number*] }	Mandatory
Configuring the idle timeout exit time.	**exec-timeout** *exec-timeout-minute_number* [*exec-timeout-second_number*]	Mandatory The default idle timeout exit time is 5 minutes.

Configure the Line Password

Use 0 and 7 to indicate whether the line password is in plain text or cipher text. 0 indicates that the password is in plain text while 7 indicates that the password is in cipher text. In interaction mode, only plain-text password is allowed. That is, in this mode, parameter value 0 is used.

Table 3-12 Configuring the Line Password

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the line configuration mode of the Console port or VTY.	**line** { **con 0** | **vty** *vty-min-number* [*vty-max-number*] }	Mandatory
Configure the line password.	**password 0** *password*	Mandatory

Configure Line Using Attributes

Set the use property of line vty to telnet or SSH. For example, if it is configured to Telnet, line vty can only be used by Telnet, but SSH cannot be used.

Table 3-13 Configure line using attributes

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the line configuration mode of vty	**line** { **vty** *vty-min-number* [*vty-max-number*] }	Mandatory
Configure the using attributes of line	**protocol input** { **all** | **ssh** | **telnet** }	Mandatory By default, the line vty is shared by ssh and telnet.

Configure the Login Authentication Mode

The device supports the following login authentication modes:

- Login password authentication mode: Uses line password authentication.
- Login aaa authentication mode: Uses the AAA authentication.
- No login indicates that no authentication is required for login.

- By default, the no login authentication mode is used for Telnet, and the local user authentication mode is used for SSH.

Table 3-14 Configuring the Login Authentication Mode

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the line configuration mode of the Console port or VTY.	**line** { **con 0** | **vty** *vty-min-number* [*vty-max-number*] }	Mandatory
Configure the login authentication mode.	**login {aaa [** *domain-name* **| default] | password}**	The command will affect the AAA authentication, authorization, and accounting.

Enable Modem Function of Console Port

Because the console port on the device has the function of the AUX port, it can realize remote dial-up login by enabling the modem function of the Console port.

Table 3-15 Enable the Modem function of the Console port

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the line configuration mode of Console port	**line con 0**	Mandatory
Enable the Modem function of the Console port	**modem auto-detection**	Mandatory By default, do not enable the Modem function of the Console port.

Configure ACL in line

Configure the access control list of IP address/IPv6 address under line.

Table 3-16 Configure ACL in line

Step	Command	Description
Enter the line configuration mode	`line vty` *vty-min-number* [*vty-max-number*]	Optional
Enter the line configuration mode of the Console port	**line con 0**	Optional
Configure the ingress ACL of the IP address	**access-class** { *access-list-number* | *access-list-name* } **in**	Optional The number of the IP standard ACL, ranging from 1 to 1000
Configure the egress ACL of the IP address	**access-class** { *access-list-number* | *access-list-name* } **out**	Optional
Configure the ingress ACL of the IPv6 address	**ipv6 access-class** { *access-list-number* | *access-list-name* } **in**	Optional The number of the IPv6 ACL, ranging from 7001 to 8000
Configure the egress ACL of the IPv6 address	**ipv6 access-class** { *access-list-number* | *access-list-name* } **out**	Optional

Configure the User Login Timeout Time

During login, if the wait time for the user to input the user name or password times out, the system prompts that the login fails. By default, the login timeout time is 30 seconds. To modify the wait timeout time, use this function.

Table 3-17 Configuring the User Login Wait Timeout Time

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the line configuration mode of the Console port.	**line con 0**	Mandatory.

Step	Command	Description
Configure the user login wait timeout time.	**timeout login respond** *respond-time-value*	Mandatory. By default, the wait time for the user to input the user name or password is 30 seconds.

3.2.5. System Control and Management Monitoring and Maintaining

Table 3-18 System Control and Management Monitoring and Maintaining

Command	Description
clear line { **con** *con-number* | **vty** *vty-number* }	Force one terminal connection to offline
show privilege	View the privilege level of the current user.
who	View the user information of the current login device

4. FTP, FTPS, TFTP AND SFTP

File Transfer Protocol (FTP) is used between a server and a client to transmit files. It improves file sharing, and provides an efficient and reliable data transmission mode between the user and remote computer. The FTP protocol usually uses TCP port 20 and 21 for transmission. Port 20 transmits data in active mode, and port 21 transmits control messages.

Similar to most Internet services, FTP uses the client/server communication mechanism. To connect to an FTP server, usually you are required to have the authorized account of the FTP server. On the Internet, a large number of FTP servers are anonymous FTP servers, which aim at provide file copying services to the public. For this type of FTP server, users need not register with the server or obtain authorization from the FTP servers.

FTP supports two types of file transmission modes:

- ASCII transmission mode, in which text files are transmitted.
- Binary transmission mode, in which program files are transmitted.

If the device acts as an FTP client and server, only use the binary transmission mode.

FTP supports two working modes:

- Active mode: An FTP client first sets up a connection with an FTP server through the TCP21 port, and sends commands through this channel. If the FTP client wants to receive data, it sends the PORT command through this channel. The PORT command contains through which port the client receives data. Then the FTP server connects its TCP20 port to the specified port of the FTP client to transmit data. The FTP server must set up a new connection with the FTP client to transmit data.
- Passive mode: The method of setting up the control channel in passive mode is similar to that in active mode. However, after the connection is set up, the PASV command instead of the PORT command is sent. After the FTP server receives the PASV command, it opens a high end port (with the port number larger than 1024) and inform the client to transmit data through this port. The FTP client connects to the port of the FTP server, and then the FTP server transmits data through this port.

Many Intranet clients cannot log in to the FTP server in active mode, because the server fails to set up a new connection with an Intranet client.

When the device acts as an FTP client, it can set up a data connection with the server in active and passive mode. When the device acts as FTP server, it is limited to SSAC mode. In strict mode, the device only supports passive mode, not active mode.

FTPS is one enhanced FTP protocol of using the standard FTP protocol and commands in the security socket layer, adding the SSL security function for the FTP protocol and data channel. FTPS is also called FTP-SSL and FTP-over-SSL. SSL is one protocol of encrypting and decrypting the data in the security connection between the client and the server with the SSL function. On the device, only the FTP client supports the function.

Trivial File Transfer Protocol (TFTP) is a simple file transfer protocol which is based on the User Datagram Protocol (UDP). It transmits data through UDP port 69. The protocol is designed for transmission of small files; therefore, it does not have as many functions as the FTP protocol. It does not support list of directories or authentication.

SFTP (Secure File Transfer Protocol /Secure FTP) is the new function in SSH 2.0. SFTP is based on the SSH connection so that the remote user can log into the device safely for managing the file, transmitting the file and other operations, providing higher security guarantee for the data transmission. SFTP provides one safe method for transmitting the file. SFTP is the sun function of SSH, realizing the safe transmission of the file. SFTP encrypts the transmitted authentication information and transmitted data, so using SFTP is safe. If the requirement for the network security is higher, you can use SFTP to replace FTP, but the SFTP file transmission adopts the encryption/decryption technology, so the transmission efficiency is lower than the FTP file transmission.

4.1. FTP, FTPS, TFTP and SFTP Function Configuration

Table 4-1 FTP and TFTP Function Configuration List

Configuration Tasks	
Configure an FTP server.	Configure the functions of an FTP server.
Configure an FTP client.	Configure the functions of an FTP client.
Configure a TFTP client.	Configure the functions of a TFTP client.
Configure a TFTP server	Configure the functions of a TFTP server
Configure an SFTP server	Configure the functions of the SFTP server
Configure an SFTP client	Configure the functions of the SFTP client

4.1.1. Configure an FTP Server

Configuration Condition

None

Configure the Functions of an FTP Server

Before configuring the device as the FTP server, first enable the FTP server function. Then, the FTP client can access the FTP server. For security sake, the device provides the FTP service only to authorized users, and it limits the maximum allowed number of concurrent login users.

Table 4–2 Configuring the Functions of an FTP Server

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the FTP server function.	**ftp enable**	Mandatory. By default, the FTP server function is disabled.
Create a manager user and enter the manager user mode	**local-user** *user-name* **class manager**	
Configure the user to support ftp service-type	**service-type ftp**	
Configure the authorized user name and password.	**password 0** *password*	Mandatory. By default, the user name and password are not configured. For details of the command, refer to the related sections in "LUM".
Configure the FTP service listening port number	**ftp listen-port** [*port-num*]	Optional By default, the FTP service listening port number is 21.
Configure the maximum allowed number of concurrent login users.	**ftp max-user-num** *user-num*	Optional. By default, the maximum allowed number of concurrent login users is 1.
Configure the connection timeout time.	**ftp timeout** *time*	Optional. By default, the connection timeout time is 300 seconds.

4.1.2. Configure an FTP Client

Configuration Condition

None

Configure the Functions of an FTP Client

On the device, when you use the **copy** command to copy files (Refer to the related sections in "File System Management") or use the **sysupdate** command to upgrade the software version (Refer to the related sections in "Software Upgrade"), the device can be triggered to act as the FTP client and set up a connection with the remote FTP server.

The connection between an FTP client and an FTP server uses the address of the outgoing interface of the route to the FTP server as the source address by default. Users can also use the **ip ftp source-address** or **ip ftp source-interface** commands to specify the FTP client source address or source interface.

Table 4-3 Configuring the Functions of an FTP Client

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the source address of the FTP client.	**ip ftp** { **source-interface** *interface-name* | **source-address** *ip-address* }	Optional. By default, the FTP client uses the address of the outgoing interface of the route to the FTP server as its source address to communicate with the FTP server.
Return to the privileged user mode	**exit**	-
Enter the file system configuration mode	**filesystem**	-
Copy the file	**copy** { *src-parameter* } { *dest-parameter* }	Optional Use this command to download or upload files with FTP server. For a detailed description of the command, please refer to the chapter "File System Management"

Step	Command	Description
Return to the privileged user mode	**exit**	-

Note:

- For the security sake, some networks may restrict the communication between the address of the outgoing interface of the route from the device to the FTP server and the FTP server, but the other service interface addresses are available. In this case, users can use the **ip ftp source-address** or **ip ftp source-interface** commands to specify the FTP client source address or source interface.

For the FTPS function, the above command is also effective.

4.1.3. Configure a TFTP Client

Configuration Condition

None

Configure the Functions of a TFTP Client

On the device, when you use the **copy** command to copy files (Refer to the related sections in "File System Management") or use the **sysupdate** command to upgrade the software version (Refer to the related sections in "Software Upgrade"), the device can be triggered to act as the TFTP client and set up a connection with the remote TFTP server.

The connection between a TFTP client and a TFTP server uses the address of the outgoing interface of the route to the TFTP server as the source address by default. Users can also use the **ip tftp source-address** or **ip tftp source-interface** commands to specify the TFTP client source address or source interface.

Table 4-4 Configuring the Functions of a TFTP Client

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the source address of the TFTP client.	**ip tftp** { **source-interface** *interface-name* | **source-address** *ip-address* }	
Return to the privileged user mode	**exit**	-
Enter the file system configuration mode	**filesystem**	-

Step	Command	Description
Copy the file	**copy** { *src-parameter* } { *dest-parameter* }	Optional By default, no files are copied. Use this command to download or upload files with TFTP server. Please refer to "file system management" for details of the command.
Return to the privileged user mode	**exit**	-
Upgrade the software version	**sysupdate** { **cmm** | **fpga** | **image** | Bootloader} [**vrf** *vrf-name*] *dest-ip-address filename*	Optional This command is used to upgrade CMM, FPGA, image and Bootloader programs from FTP server through device interface. For a detailed description of the command, please refer to the section "software upgrade"

Note:

- For the security sake, some networks may restrict the communication between the address of the outgoing interface of the route from the device to the TFTP server and the TFTP server, but the other service interface addresses are available. In this case, users can use the **ip tftp source-address** or **ip tftp source-interface** commands to specify the TFTP client source address or source interface

4.1.4. Configure a TFTP Server

Configuration Condition

None

Configure the Functions of a TFTP Server

To configure a device as the TFTP server, first enable the TFTP server function so that the TFTP client can access.

Table 4-5 Configuring the Functions of a TFTP Server

Step	**Command**	**Description**
Enter the global configuration mode.	**configure terminal**	-
Enable the functions of the TFTP server	**tftp enable**	Mandatory By default, do not enable the functions of the TFTP server.

4.1.5. Configure an SFTP Server

Configuration Condition

None

Configure the Functions of an SFTP Server

Before configuring the device as the SFTP server, first enable the SFTP server function. Then, the SFTP client can access the SFTP server. SFTP is one subsidiary function of SSH, so the configuration of enabling the SFTP service is the same as that of enabling the SSH remote login service.

Table 4-6 Configuring the SFTP server function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the SFTP server function	**ip ssh server** [**sshv1-compatible**] **[** *listen-port* **]**	Mandatory By default, do not enable the SFTP server function.

4.1.6. Configure a SFTP Client

Configuration Condition

None

Configure the Functions of an SFTP Client

The device serves as the SFTP client and connects the SFTP server, downloading the file from the SFTP server or uploading the file to the SFTP server.

Table 4-7 Configuring the function of an SFTP client

Step	Command	Description
Configure the device as the SFTP client to upload or download the file to the SFTP server	**sftp { get | put }** [**vrf** *vrf-name*] *host-ip-address port-number* [**source-interface** *interface-name*] *user password src-filename dest-filename* [compress]	Optional

4.1.7. FTP, TFTP and SFTP Monitoring and Maintaining

None

4.2. Typical Configuration Example of FTP and TFTP

4.2.1. Configure a Device as an FTP Client

Network Requirements

- A PC acts as an FTP server, and Device acts as an FTP client. The network between the server and the device is normal.
- On the FTP server, the user name for a device to log in to the FTP server is admin, and the password is admin. The files to be downloaded are placed in the FTP server directory.
- The device acts as the FTP client to upload files to and download files from the FTP server.

Network Topology

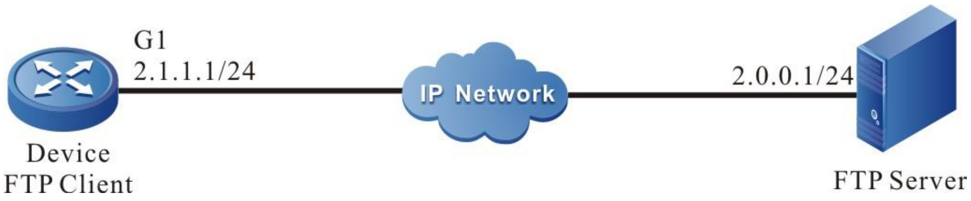


Figure 4-1 Networking for Configuring a Device as an FTP Client

Configuration Steps

Step 1: Configure an FTP server, and place the files to be downloaded in the FTP server directory. (Omitted)

Step 2: Configure the IP addresses of the devices so that the network between the client and the server is normal. (Omitted)

Step 3: Device acts as the FTP client to upload files to and download files from the FTP server.

#In the global mode of the Device, copy one file from the FTP server to the file system of Device.

```
Device>enable
  Device# copy ftp 2.0.0.1 admin admin rplh-g-6.3.31(36).pck file-system rplh-g-6.3.31(36).pck
```

#In the file system mode of Device, copy one file from the FTP server to the file system of Device.

```
Device#filesystem
Device (config-fs)#copy ftp 2.0.0.1 admin admin rplh-g-6.3.31(36).pck file-system rplh-g-6.3.31(36).pck
```

#In the file system mode of Device, copy the startup file of Device into the FTP server.

```
Device#filesystem
Device(config-fs)#copy file-system startup ftp 2.0.0.1 admin admin startup.txt
```

Step 4: Check the result.

#After the copy process is completed, check whether the downloaded file exists in the file system of Device. In the FTP server, check whether the uploaded file exists. (Omitted)

```
Device#filesystem
Device(config-fs)#dir


Directory of /flash:


Size          Date        Time          Name
------------   ------     ------        --------
2            Jul-16-2020  16:16:34       PKISTORE
204725        Oct-20-2020  16:09:29       history
4096          Jul-04-2018  14:30:55  <DIR>  netconf
4096          Jul-03-2017  08:57:01  <DIR>  snmp
53327         Sep-08-2020  10:44:52       startup
4096          Dec-29-2018  16:55:59  <DIR>  tech
4096          Jun-11-2020  15:23:11  <DIR>  webs
34693796       Sep-05-2019  11:05:33       rplh-g-6.3.31(36).pck
```

Note:

- If the " FTP Hookup: connect error 65" message is printed, it indicates that the server cannot be reached, and the cause may be that the route is not available or the server has not been started.
- If the " Total 51054 bytes copying completed!" message is printed, it indicates that the file is copied successfully and the file size displayed by the printed information is related with the actual size of the file.

4.2.2. Configure a Device as an FTP Server

Network Requirements

- Device1 acts as an FTP server, while PC and Device2 act as FTP clients. The network between the client and the server is normal.
- On the FTP server Device1, the user name is admin, and the password is admin. The file system directory of Device1 acts as the root directory of the FTP server.
- PC and Device2 act as the FTP client to upload files to and download files from the FTP server Device1.

Network Topology

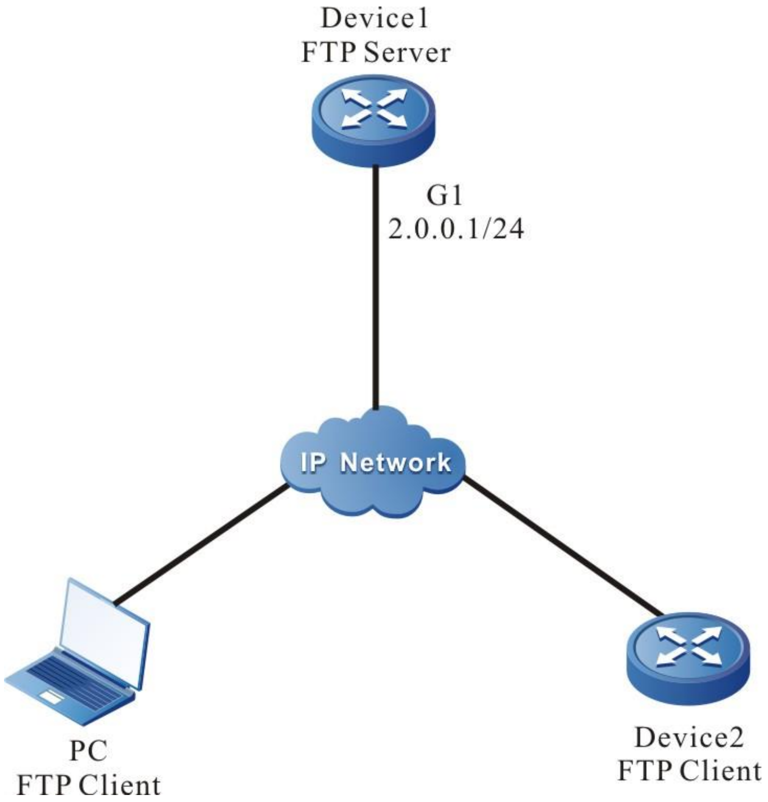


Figure 4–2 Networking in Which a Device Acts as an FTP Server

Configuration Steps

Step 1: Configure the IP addresses of the devices so that the networks between the PC, Device 2, and Device 1 are normal. (Omitted)

Step 2: On the FTP server Device1, enable the FTP service, and configure the authorized user name and password.

#On Device1, enable the FTP service, and configure the authorized user name and password.

```
Device1#configure terminal
Device1(config)#local-user admin1 class manager
Device1(config-user-manager-admin1)#service-type ftp
Device1(config-user-manager-admin1)#password 0 admin2
Device1(config-user-manager-admin1)#exit
```

#On thw FTP server Device1, enable the FTP service.

```
Device1#configure terminal .
Device1(config)#ftp enable
```

#On the FTP server Device1, set the maximum number of concurrent users to 2.

```
Device1#configure terminal .
Device1(config)#ftp max-user-num 2
```

Step 3: Check the result.

#Check whether the FTP service function is enabled on Device1.

```
Device1#show  ip sockets
Active Internet connections (including servers)
PCB      Proto Recv-Q Send-Q  Local Address        Foreign Address       vrf      (state)
-------- ----- ------ ------  --------------------- ---------------------- ----
---   -------
701bb4a4 TCP       0      0  0.0.0.21            0.0.0.0             all       LISTEN
767e4e24 TCP       0      0  0.0.0.23            0.0.0.0             all       LISTEN
767e4464 TCP      0     0  127.0.0.1.2600      127.0.0.1.1024      global    ESTABLISHED
75f44f04 TCP      0     0  127.0.0.1.1024      127.0.0.1.2600      global    ESTABLISHED
75f44e44 TCP       0     0  127.0.0.1.2600      0.0.0.0             global    LISTEN
767e4524 UDP       0      0  0.0.0.514          0.0.0.0             all
767e4824 UDP       0      0  0.0.0.1025         0.0.0.0             all
75f44b44 UDP       0      0  0.0.0.1024         0.0.0.0             all
```

If the FTP service function has enabled, you can find that port 21 is in the listen state.

Step 4: Use Device2 as an FTP client to copy a startup file from FTP server Device1 to Device2.

```
Device2#filesystem
Device2(config-fs)#copy ftp 2.0.0.1 admin1 admin2 startup file-system startup
```

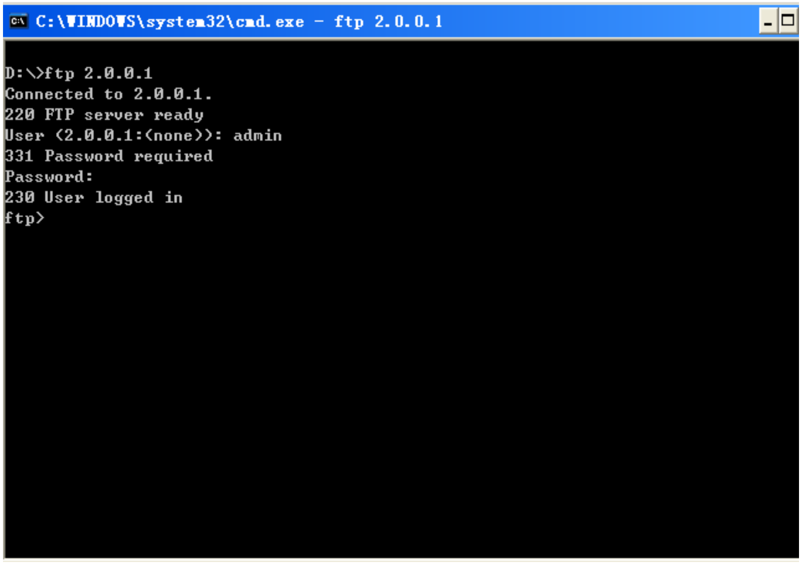
Step 5: Use PC as an FTP client to copy a startup file from FTP server Device1 to PC.

#In the following part, the Windows DOS screens are taken as an example to illustrate the process.

#In the Windows DOS screen, input the correct IP address, user name, and password to log in to the FTP server.

```
D:\>ftp 2.0.0.1
Connected to 2.0.0.1.
220 FTP server ready
User (2.0.0.1:(none)): admin1
331 Password required
```

```
Password:
230 User logged in
ftp>
```

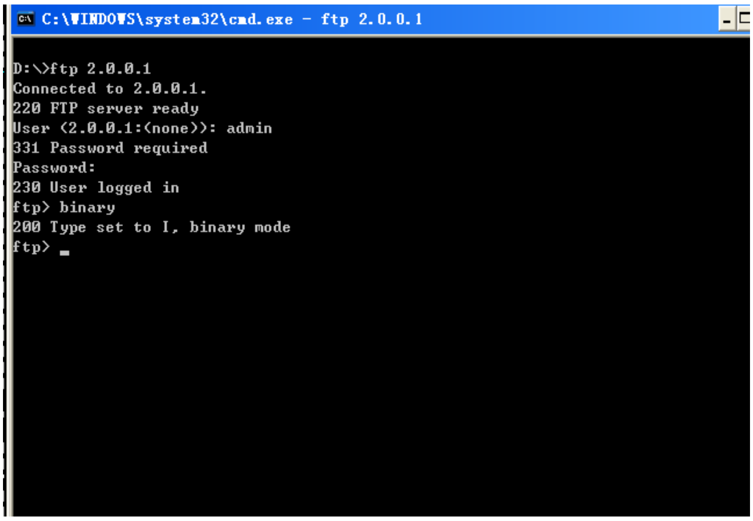


```
D:\>ftp 2.0.0.1
Connected to 2.0.0.1.
220 FTP server ready
User (2.0.0.1:(none)): admin
331 Password required
Password:
230 User logged in
ftp>
```

Figure 4-3 Logging in to the FTP Server via the Windows DOS Screen

#Configure the PC and FTP server to transmit data in binary mode.

```
ftp>binary
```

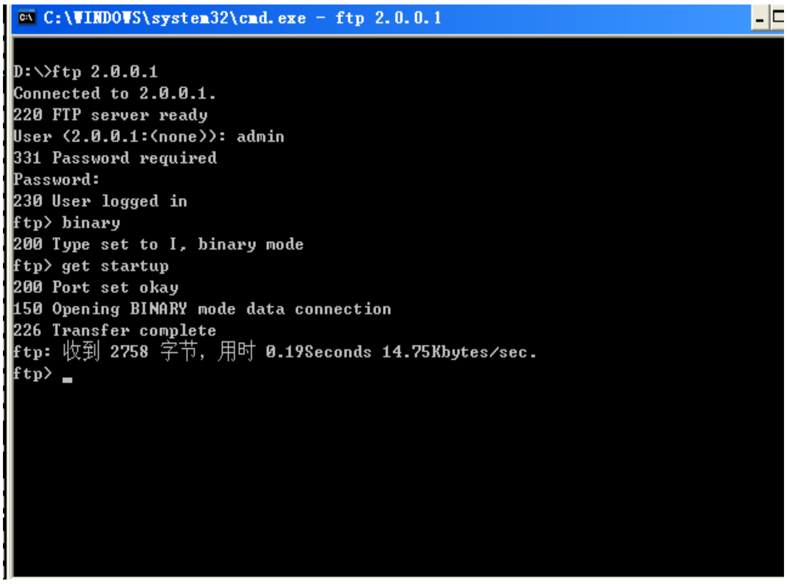


```
D:\>ftp 2.0.0.1
Connected to 2.0.0.1.
220 FTP server ready
User (2.0.0.1:(none)): admin
331 Password required
Password:
230 User logged in
ftp> binary
200 Type set to I, binary mode
ftp> _
```

Figure 4-4 Configuring the PC and FTP Server to Transmit data in Binary Mode

#Obtain the startup file in the file system of the FTP server Device1.

```
ftp>get startup
```



```
D:\>ftp 2.0.0.1
Connected to 2.0.0.1.
220 FTP server ready
User (2.0.0.1:(none)): admin
331 Password required
Password:
230 User logged in
ftp> binary
200 Type set to I, binary mode
ftp> get startup
200 Port set okay
150 Opening BINARY mode data connection
226 Transfer complete
ftp: 收到 2758 字节, 用时 0.19Seconds 14.75Kbytes/sec.
ftp> _
```

Figure 4-5 Copying a Configuration File from the FTP Server

After the file copy process is completed, the file is available in the specified Windows directory.

Note:

- If the "421 Session limit reached, closing control connection" message is printed, it indicates that the number of connections has exceeds the maximum number allowed by the server.
- When you use a device to copy a file, if the " FTP Hookup: connect error 61 Error: Getting response from FTP server failed " message is printed, the cause may be that the server function is not enabled, or the route between the server and the client is not reachable.
- When you connect the FTP server through the FTP client PC, if the " connect :Unknown error number" is printed, the cause may be that the server function is not enabled, or the route between the server and the client is not reachable.

4.2.3. Configure a Device as an TFTP Client

Network Requirements

- A PC acts as a TFTP server, and Device acts as a TFTP client. The network between the server and the device is normal. The files to be downloaded are placed in the TFTP server directory.
- The device acts as the TFTP client to upload files to and download files from the TFTP server.

Network Topology

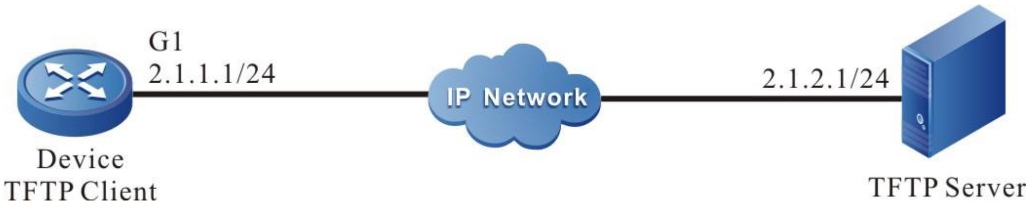


Figure 4-6 Networking for Configuring a Device as a TFTP Client

Configuration Steps

Step 1: Enable the TFTP server function on PC, and place the files to be downloaded in the TFTP server directory. (Omitted)

Step 2: Configure the IP addresses of the interfaces so that the network between the client and the server is normal. (Omitted)

Step 3: Device acts as the TFTP client to upload files to and download files from the TFTP server.

#On Device, copy a file from the TFTP server to the file system of Device.

```
Device#filesystem
Device(config-fs)#copy tftp 2.1.2.1 rplh-g-6.3.31(36).pck file-system rplh-g-6.3.31(36).pck
```

#On Device, copy the startup file from Device to the TFTP server.

```
Device#filesystem
Device(config-fs)#copy startup-config tftp 2.1.2.1 startup.txt
```

Step 4: Check the result.

After the copy process is completed, check whether the downloaded file exists in the file system of Device. In the TFTP server, check whether the uploaded file exists. (Omitted)

```
Device#filesystem
Device (config-fs)#dir
  size      date       time      name
--------    ------    ------   --------
102180    OCT-26-2012  08:44:02  logging
68624     OCT-25-2012  16:59:16  startup
9266      FEB-29-2012  14:21:16  history
1024      DEC-20-2011  17:42:28  snmp           <DIR>
34693796  SEP-07-2012  15:24:18  rplh-g-6.3.31(36).pck
```

Note:

- If the " Total 51054 bytes copying completed!" message is printed, it indicates that the file copy is successful. The message shows the file size, which is determined by the actual file size.
- When you use a device to copy a file, if the " tftpSend: Transfer Timed Out.Error: Tftp transmit error " message is printed, the cause may be that the TFTP server function is not enabled, or the route between the server and the client is not reachable.

5. FILE SYSTEM MANAGEMENT

5.1. Overview

The following lists the storage medium of the device and their functions:

- SDRAM: Synchronous Dynamic Random Access Memory (SDRAM) provides the space for executing application programs of the device.
- FLASH: Stores application programs, configuration files, and the BootROM programs, and so on.
- EEPROM: Electrically Erasable and Programmable Read-Only Memory (EEPROM) stores system configuration files and user information which is frequently changed.
- SD card: Used to save user data
- USB: Used to save the user data.

The device manages the following types of files:

- BootROM files: Store basic data for system initialization.
- Device application programs: Implement tasks such as route forwarding, file management, and system management.
- Configuration files: Store the system parameters that are configured by the users.
- Log files: Stores system log information.

Note:

- The filesystem command is used to enter the file system, and can be used on both the master control and standby control.

5.2. File System Management Function Configuration

Table 5-1 File System Management Function List

Configuration Tasks	
Manage storage devices.	Display the information about a storage device.
	Format a storage device.
Manage file directories.	Display the information about a file directory.
	Display the current working path.
	Change the current working path.
	Create a directory.
	Delete a directory.

Configuration Tasks	
Manage file operations	Copy a file.
	Rename a file.
	Display the content of a file.
	Delete a file.
Execute a configuration file manually.	Execute a configuration file manually.
Configure startup parameters.	Configure startup parameters.

5.2.1. Manage Storage Devices

Configuration Condition

Before performing operations on storage devices, ensure that:

- The system has started normally.

Display the Information about a Storage Device

By displaying the information about a storage device, you can view the features of the storage device and the size of the remaining space.

Table 5-2 Displaying the Information about a Storage Device

Step	Command	Description
Enter the file system configuration mode.	**filesystem**	-
Display the information about a storage device.	**volume**	Mandatory

Note:

- The **volume** command is a command under the file system, which can be used on both the master and slave MPU file systems.

Format the Storage Devices

If the file system of a storage device is damaged and as a result, the storage device is unavailable, you can use the format command to format the storage device.

Table 5-3 Formatting a Storage Device

Step	Command	Description
Enter the file system configuration mode.	**filesystem**	-
Format a storage device.	**format {/flash | /syslog | /usb* | /sdcard*}**	Optional

Caution:

- Exercise caution in formatting a storage device, because the operation may cause permanent loss of all files on the storage device, and the files cannot be recovered.

5.2.2. Manage File Directories

Configuration Condition

None

Display the Information about a File Directory

By displaying the information about a file directory, you can view the details of the files in the specified directory.

Table 5-4 Displaying the Information About a File Directory

Step	Command	Description
Enter the file system configuration mode.	**filesystem**	-
Display the information about a directory.	**dir** [*path*]	Mandatory

Note:

- The **dir** command is a command under the file system, which can be used on both the master and slave MPU file systems.

Display the Current Working Path

By displaying the current working path, you can view the details of the current path.

Table 5-5 Displaying the Current Working Path

Step	Command	Description
Enter the file system configuration mode.	**filesystem**	-
Display the current working path.	**pwd**	Mandatory

Note:

- The **pwd** command is a command under the file system, which can be used on both the master and slave MPU file systems.

Change the Current Working Path

By changing the current working path, you can switch over a user to the specified directory.

Table 5-6 Changing the Current Working Path

Step	Command	Description
Enter the file system configuration mode.	**filesystem**	-
Change the current working path.	**cd** *path*	Mandatory

Note:

- The **cd** command is a command under the file system, which can be used on both the master and slave MPU file systems

Create a Directory

If you want to create a directory in the file system, perform this operation.

Table 5-7 Creating a Directory

Step	Command	Description
Enter the file system configuration mode.	**filesystem**	-
Create a directory.	**mkdir** *directory*	Mandatory

Note:

- The **mkdir** command is a command under the file system, which can be used on both the master and slave MPU file systems.

Delete a Directory

The **rmdir** command is used to remove the specified directory in the file system.

After entering the command, if the directory is empty, it will be deleted directly; If the directory is a non-empty directory, you need to enter the forced delete parameter [*force*]. When you use **rmdir** to force to delete the specified directory, the subdirectory in the directory and the files in the directory will be deleted together.

Table 5-8 Deleting a Directory

Step	Command	Description
Enter the file system configuration mode.	**filesystem**	-
Delete a directory.	**rmdir** { *directory* } **[***force***]**	Mandatory

Note:

- The **mkdir** command is a command under the file system, which can be used on both the master and slave MPU file systems.
- Exercise caution when deleting a directory, because the operation of deleting the directory may permanently delete all sub-directories and files in the directory, and the files cannot be recovered.

5.2.3. Manage File Operations

Configuration Condition

None

Copy a File

In the file system, you can copy a file to the specified directory.

Table 5-9 Copying a File

Step	Command	Description
Enter the file system configuration mode.	**filesystem**	-
Copy a file.	**copy** *src-parameter dest-parameter*	Mandatory

Note:

- The **copy** command can be used to copy files between the active and standby file systems, the FTP server, and the TFTP server. For details, refers to the description of the **copy** command in the technical manual.

Rename a File

In the file system, you can change the name of a file into a specified name.

Table 5-10 Renaming a File

Step	Command	Description
Enter the file system configuration mode.	**filesystem**	-
Rename a file.	**rename** { *src-filename* } { *dest-filename* }	Mandatory Both the active and standby file systems can use the command.

Note:

- The **rename** command is a command under the file system, which can be used on both the master and slave MPU file systems.

Display the Content of a File

In the file system, you can view the content of a file.

Table 5-11 Displaying the Content of a File

Step	**Command**	**Description**
Enter the file system configuration mode.	**filesystem**	-
Display the content of a file.	**type** { *path/filename* }	Mandatory

Note:

- The **type** command is a command under the file system, which can be used on both the master and slave MPU file systems.

Delete a File

In the file system, you can delete a file that is no longer in need.

Table 5-12 Deleting a File

Step	**Command**	**Description**
Enter the file system configuration mode.	**filesystem**	-
Delete a file.	**delete** { *path/filename* }	Mandatory

Note:

- The **delete** command is a command under the file system, which can be used on both the master and slave MPU file systems.
- Exercise caution when you use the delete command because it permanently deletes a file, and the file cannot be recovered.
- For non-hidden files, please fully understand its function before performing file deletion operation to avoid mistakenly deleting important files.

5.2.4. Execute Configuration Files Manually

Configuration Conditions

Before executing the configuration file manually, first complete the following task:

- The system started manually.is

Execute Configuration Files Manually

Execute the configuration file manually, and you can load the configuration file of the specified path.

Table 5-13 Execute the configuration file manually

Step	Command	Description
Enter the file system configuration mode.	**filesystem**	-
Execute the configuration file manually	**config-file** { *path/filename* } [**debug**]	Optional

Note:

- Please use it cautiously when you manually execute the configuration file. It will force the current configuration of the system to be modified, which may affect the business of the system. By default, the startup configuration file has been loaded during system startup.

5.2.5. Configure Startup Parameters

Configuration Condition

None

Configure Startup Parameters

In configuring startup parameters, you can configure the application program file that is to be used in next startup.

Table 5-14 Configuring Startup Parameters

Step	**Command**	**Description**
Enter the file system configuration mode.	**filesystem**	-
Configure startup parameters.	**boot-loader** *path/filename* [*bootline-number*]	Mandatory Both the active and standby file systems can use the command.

5.2.6. File System Managing, Monitoring, and Maintaining

Table 5-15 File System Managing, Monitoring, and Maintaining

Command	Description
clear { **boot-loader** } [*bootline-number*]	Clears the startup parameters with the specified index.
show filesystem	Display the information about the file system.
show filesystem device	Display the storage device information in the system
show fsp watchers	Display the monitoring status of the storage device
show file location	Display the storage location information of the system file in the file system
show boot-loader	Display the system startup parameters.
file-system utilization warner-threshold value threshold { /flash | /syslog | /usb* | sdcard***}**	It is used to set the space monitoring threshold of all the storage devices supported by flash, syslog, USB and sdcard, and enable the space monitoring function of the device. By default, only /flash is monitored, and the alarm threshold is 5% of the total size of /flash space. If 5% of the total size of /flash space is greater than 64MB, the alarm threshold value is 64MB.

5.3. Typical Configuration Example of File System Management

5.3.1. Configure Startup Parameters

Network Requirements

None

Network Topology

None

Configuration Steps

Step 1: Enter the file system configuration mode.

Step 2: Configure system startup options.

#Configure the system startup parameters.

```
Hostname #filesystem
Hostname(config-fs)#show boot-loader
The app to boot at the next time is:
The app to boot at the this time is: flash0: /flash/rp32-8.2.0.130(R).pck

Boot-loader0: flash0: /flash/rp32-8.2.0.130(R).pck
Boot-loader4: backup0: rp32-8.2.0.130(R).pck
```

#The next boot file in the system is changed to rp32-8.2.0.131(R).pck file stored in flash, and the priority is set to 0.

```
Hostname #filesystem
Hostname(config-fs)#boot-loader /flash/rp32-8.2.0.131(R).pck 0
```

#View the configuration result.

```
Hostname #filesystem
Hostname(config-fs)#show boot-loader
The app to boot at the next time is: flash0: /flash/rp32-8.2.0.131(R).pck
The app to boot at the this time is: flash0: /flash/ rp32-8.2.0.130(R).pck

Boot-loader0: flash0: /flash/rp32-8.2.0.131(R).pck
Boot-loader4: backup0: rp32-8.2.0.130(R).pck
```

5.3.2. Configure Monitoring Storage Device Space

Network Requirements

None

Network Topology

None

Configuration Steps

Step 1: Enter the global configuration mode

Step 2: Configure monitoring the space of the storage device.

# Configure monitoring the /syslog space.

```
Hostname #configure terminal
Hostname(config)#file-system utilization warner-threshold value 100 /syslog
```

#View the configuration result.

```
Hostname #show fsp watchers
device          threshold(MB)     status
/flash          100               valid
/syslog          100               valid
```

6. CONFIGURATION FILE MANAGEMENT

6.1. Overview

Configuration file management is a function that is used to manage device configuration files. Through the command line interface provided by the device, users can easily manage configuration files. If the device needs to automatically load the current configuration of users after restart, the current configuration commands must be saved into the configuration file before the device restarts. Users can upload configuration files to or download configuration files from another device through FTP or TFTP, realizing batch device configuration. The device configuration is categorized into the following two types:

Startup configuration:

When the device starts, it loads the startup configuration file with the name "startup" by default, and it completes the initialization configuration of the device. This configuration is called startup configuration. Here the device has two startup configuration files, one is the default startup configuration file, and the other is the backup startup configuration file. When the device starts, if the default startup configuration file does not exists, the system copies the backup startup configuration file to the location of the default startup configuration file and loads this startup configuration file.

Current configuration:

Current configuration is a set of commands that take effect currently. It consists of startup configuration and the configuration that is added or modified by the user after startup. The current configuration is saved in the memory database. If the current configuration is not saved into the startup configuration file, the configuration information gets lost after the device restarts.

The following describes the contents and formats of the configuration files:

- Configuration files are saved in the file system in the form of text files.
- The contents of the configuration files are saved in the form of configuration commands, and only non-default configuration is saved.
- Configuration files are organized based on command modes. All commands in one command mode are organized together to form a paragraph.
- Paragraphs are organized according to a certain rule: system configuration mode, interface configuration mode, and configuration modes of different protocols.
- Commands are organized according to their relations. The related commands form a group, and different groups are separated by blank lines.

6.2. Configuration File Management Function Configuration

Table 6-1 Configuration File Management List

Configuration Tasks	
Save the current configuration.	Save the current configuration.
Back up device configuration.	Back up the current configuration.
	Back up the startup configuration.
Restore the startup configuration.	Restore the startup configuration.

6.2.1. Save the Current Configuration

Configuration Condition

None

Save the Current Configuration

If the current configuration of the user can take effect only after the device starts, you need to save the current configuration into the startup configuration file. When saving the current configuration, the active master controller and the standby master controller will save the current configuration to the specified configuration file at the same time, so as to ensure that the contents of the configuration files of the active master controller and the standby master controller are consistent.

Table 6-2 Saving the Current Configuration

Step	Command	Description
Save the current configuration to the startup configuration file.	**write**	Mandatory

Note:

- If the device is restarted or powered off while the configuration file is being saved, configuration information may get lost.
- Saving the current configuration not only saves the configuration to the startup configuration file, but also saves the configuration to the backup startup configuration file.

6.2.2. Configure the Backup System

Configuration Condition

Before configuring the backup system parameters, ensure that:

- The route between the device and the server is reachable.
- The configuration file to be backed up exists; otherwise, backup fails.

Back Up the Current Configuration

In backing up the current configuration, you can use a command to back up the current configuration to the FTP server.

Table 6-3 Backing Up the Current Configuration

Step	Command	Description
Enter the privileged configuration mode.	**enable**	-
Back up the current configuration to a remote host through the FTP protocol.	**copy running-config ftp** *ip-address username password dest-filename*	Mandatory

Back Up Startup Configuration

In backing up the startup configuration, you can use a command to back up the startup configuration to the FTP server.

Table 6-4 Backing Up the Startup Configuration

Step	Command	Description
Enter the privileged configuration mode.	**enable**	-
Save the startup configuration to a remote host through the FTP protocol.	**copy startup-config ftp** *ip-address username password dest-filename*	Mandatory

6.2.3. Restore the Startup Configuration

Configuration Condition

Before restoring the startup configuration, ensure that:

- The route between the device and the server is reachable.

- The configuration file that is to be restored exists.

Restore the Startup Configuration

In restoring the startup configuration, you can use a command to download the startup configuration file from the FTP server to the device and set it as the startup configuration file that is used after the active master and the standby master restart. In this way, after the device is restarted, the device can load the startup configuration file.

Table 6-5 Restoring the Startup Configuration

Step	Command	Description
Enter the privileged configuration mode.	**enable**	-
Restore the startup configuration.	**copy ftp** *ip-address username password src-filename* **startup-config**	Mandatory

Note:

- Before overwriting the local startup configuration, ensure that the configuration file matches the device type and matches the current system version.
- After performing the operation of restoring the startup configuration, the current configuration is not changed. After the device is restarted, the startup configuration is restored.

6.2.4. Configuration File Encryption

Configuration Condition

Before configuring the boot file encryption, first complete the following task:

- Whether the media on which the key file is stored exists.

Configuration File Encryption

Configuration file encryption is mainly used to encrypt the current configuration and then, write it to startup to save it, so as to avoid the disclosure of key information. The configuration file encryption function requires the existence of the media used to store the key. When this function is enabled, the current configuration will not be encrypted. Only when the configuration is saved can the configuration be encrypted. For saving the current configuration, please refer to section 6.2.1.

Table 6-6 Configure configuration file encryption

Step	Command	Description
Enter the global configuration file	**configure terminal**	-
Encrypt the configuration file	**service encryption startup algorithms SMV4 key** *password*	Mandatory Password is the password used by encryption.

Note:

- The existing startup file will not be encrypted during configuration.
- After the configuration is completed, subsequent write equivalent operations will save the configuration in the form of encryption. The encrypted configuration will still be displayed in clear text when the device key exists. When the key does not exist, the startup information will not be displayed.

6.2.5. Set Boot Configuration File

Configuration Condition

Before setting the boot configuration file, first complete the following task:

- The boot configuration file to be set exists and is legal.

Set Boot Configuration File

Setting startup configuration file is mainly used to set the configuration file or other configuration files backed up on the device as the startup configuration file used by the device next time.

Table 6-7 Set boot configuration file

Step	Command	Description
Enter the file system configuration mode	**filesystem**	-
Set the boot configuration file	**boot-startup** *startup-bak*	Mandatory startup-bak is the specified boot configuration file.

Note:

- After configuring the command, you can use the **show boot-startup** command to view whether the configuration is successful.
- After the configuration is successful, the device will load the configuration with this file as the startup configuration file for the next boot.

6.2.6. Configuration File Managing, Monitoring, and Maintaining

Table 6-8 Configuration File Managing, Monitoring, and Maintaining

Command	Description
show running-config [**after-interface** | **before-interface | interface** [*interface-name*] | [*configuration*]] [| { { **begin** | **exclude | include** } *expression* | **redirect** { **file** *file-name* | **ftp | ftps** [**vrf** *vrf-name*] { *hostname* | *ip-address* } *user-name password file-name* [VerifyType { none | peer }]} }]	Display the current configuration information.
show startup-config [| { { **begin** | **exclude** | **include** | **redirect** } *expression* } | **redirect** { **file** *filename* | **ftp** | ftps { [**vrf** *vrf-name*] { *hostname* **|** *ip-address* } *user-name password file-name* [VerifyType { none | peer }]} }]	Display the startup configuration information.

7. SYSTEM MANAGEMENT

7.1. Overview

- Through system management, users can query the current working status of the system, configure basic function parameters of the device, and perform basic maintenance and management operations on the device. The system management functions include: Configuring the device name
- Configuring the system time and time zone
- Configuring the login welcome message
- Configuring the system exception processing mode
- Restarting the device
- Configuring the password encryption service
- Configuring the history command saving function
- Configuring the login security service
- Configuring CPU monitoring
- Configuring display of properties in pages

7.2. System Management Function Configuration

Table 7-1 System Management Function List

Configuration Tasks	
Configure the device name.	Configure the device name.
Configure the system time and time zone.	Configure the system time and time zone.
Configure the login welcome message.	Configure the login welcome message.
Configure the system exception processing mode.	Configure the system exception processing mode.
Configure to restart the device.	Configure to restart the device.
Configure the history command saving function.	Configure the history command saving function.

Configuration Tasks	
Configure the login security service.	Configure the login security service.
Configure CPU monitoring.	Configure CPU monitoring.
Configure display of properties in pages.	Configure display of properties in pages.
Configure memory usage alarm threshold	Configure memory usage alarm threshold
Configure low memory usage threshold	Configure low memory usage threshold
System management monitoring and maintaining	System management monitoring and maintaining

7.2.1. Configure the Device Name

Configuration Condition

None

Configure the Device Name

A device name is used to identify a device. A user can change the device name according to the actual requirement. The modification takes effect immediately, that is, the new device name is displayed in the next system prompt.

Table 7-2 Configuring the Device Name

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the device name.	**hostname** *host-name*	Mandatory

7.2.2. Configure the System Time and Time Zone

Configuration Condition

None

Configure the System Time and Time Zone

The system time and time zone is the time displayed in the timestamp of system information. The time is determined by the configured time and time zone. You can run the **show clock** command to view the time information of the system. To make the device work normally with other devices, the system time and time zone must be accurate.

Table 7-3 Configuring the System Time and Time Zone

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the system time.	**clock timezone** *timezone-name-string hour-offset-number* [*minute -offset-number*]	Mandatory. The default is Universal Time Coordinated (UTC).
Enter the privileged user mode.	**exit**	-
Configure the system time.	**clock** *year-number* [*month-number* [*day-number* [*hour-number* [*minute-number* [*second-number*]]]]]	Mandatory

7.2.3. Configure the Login Welcome Message

Configuration Condition

None

Configure the Login Welcome Message

When a user logs in to the device for login authentication, the login welcome message is displayed. The welcome message can be configured according to the requirement.

Table 7-4 Configuring the Login Welcome Message

Step	**Command**	**Description**
Enter the global configuration mode.	**configure terminal**	-
Configure the login welcome message.	**banner motd** *banner-line*	Mandatory

7.2.4. Configure the System Exception Processing Mode

Configuration Condition

None

Configure the System Exception Processing Mode

When a system exception occurs, the system directly restarts to restore the system. To configure system exception processing mode, enable periodical exception detection and the system periodically detects the task status, code segment, and semaphore dead lock with a cycle of 10s, 10s, and 30s respectively.

Table 7-5 Configuring the System Exception Processing Mode

Step	**Command**	**Description**
Enter the global configuration mode.	**configure terminal**	-
Configure the mode of processing the abnormality	**exception** { **period-detect enable | reboot | detect-health {ignore | reload}**}	Mandatory. By default, the periodical abnormal detection is enabled.

7.2.5. Configure to Restart a Device

Configuration Condition

None

Restart a Device

When a device fault occurs, you can choose to restart the device according to the actual situation so as to eliminate the fault. The device restart modes include cold restart and hot restart. In a cold restart, the user can directly power off the device and power on the device again. In a hot restart, the user restarts the device by using a restart command. During the hot restart process, the device is not powered off.

Table 7-6 Restarting a Device

Step	Command	Description
Use a command to restart the device	**reload**	Mandatory

Note:

- If you forcedly power off and restart a device that is in the operating status, hardware damage or data loss may be caused. Therefore, this restart mode is usually not recommended.
- If you use the reload command to restart the device, all the services of the device are interrupted. Exercise caution when performing this operation.

7.2.6. Configure the History Command Saving Function

Configuration Condition

None

Configure the History Command Saving Function

Through the history command saving function, you can query and collect the history commands that have been executed. By default, it is saved in the flash file system.

Table 7-7 Configuring the History Command Saving Function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure to save history commands.	**shell-history save**	Mandatory. By default, the history command saving function is enabled.

7.2.7. Configure the Login Security Service

Configuration Condition

None

Enable the System Login Security Service

To enhance the system security, the device provides the system login security service function. The functions include:

- Prevents brute force cracking of user login passwords.
- Prevents the fast connection function.

The function of brute force cracking prevention prevents malicious illegal users from forcedly cracking the user name and password for logging in to the device. If the system finds that the number of continuous login authentication failures of a user reaches the number specified by the system, the system rejects the login request from the IP address or the login request from the user within the specified period of time.

The function of preventing fast connections prevents illegal users from initiating a large number of login requests within a short period time because this may occupy a lot of system and network resources. If the number of repeated login connections from a user reached a specified number, the system rejects the login connection requests from the IP address within the specified period of time.

Table 7-8 Enabling the System Login Security Service

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the system login security service.	**service login-secure { telnet | ssh | ftp | snmp}**	Mandatory. By default, the system login security service is enabled.

Configure the Parameters of the System Login Security Service

Table 7-9 Configuring the Login Security Service Parameters of Telnet, SSH, FTP module IP address

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the login time of the IP address forbidden by the Telnet, SSH, FTP module	**login-secure {telnet | ssh | ftp }ip-addr forbid-time** *forbid-time-number*	Mandatory By default, it is 10 minutes.
Configure the maximum successive login authentication failure times of the IP address forbidden by the Telnet, SSH, FTP module	**login-secure {telnet | ssh | ftp } ip-addr max-try-time** *max-try-time-number*	Mandatory By default, it is 5 times.
Configure the age time of the information recorded by the IP address forbidden by the Telnet, SSH, FTP module	**login-secure {telnet | ssh | ftp } ip-addr record-aging-time** *record-aging-time-number*	Mandatory By default, it is 15 minutes.

Table 7-10 Configure the login security service parameters of SNMP module community name

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the prohibited login time of the illegal community name of the SNMP module	**login-secure snmp community forbid-time** *forbid-time-number*	Mandatory By default, it is 10 minutes.
Configure max. prohibited successive login authentication failure times of the illegal community name of the SNMP module	**login-secure snmp community max-try-time** *max-try-time-number*	Mandatory By default, it is five times.
Configure the age time of the recorded information of the illegal community name prohibited by the SNMP module	**login-secure snmp community record-aging-time** *record-aging-time-number*	Mandatory By default, it is 15 minutes.

Note:

- The configuration commands of user, IP address and quick login are the same.
- **forbid-time** is the time when the user or IP address is forbidden to be silent after reaching the maximum number of authentication failures.
- **max-try-time** indicates the maximum number of authentication attempt failures of the user or IP address. After the authentication failures reach the maximum times, the login will be prohibited.
- **record-aging-time** indicates the time that the record is aged after the user or IP address authentication attempt fails. That is, how long the failure record will be cleared.
- The **restrict-interval** parameter is used to set the interval of quick login. That is, if the interval between two logins is less than or equal to the **restrict-interval**, it is considered as a fast login.

7.2.8. Configure CPU Monitoring

Configuration Condition

None

Configure CPU Monitoring

Through CPU monitoring, the system monitors the CPU occupancy to learn the current operation status of the CPU. The following shows the contents of CPU monitoring:

- Monitors the CPU occupancy of each process. After spy cpu is configured, you can view the related information by using the **show cpu** command.
- Enables the history statistics function of the CPU occupancy. After monitor cpu is configured, you can view the related information by using the **show cpu monitor** command.

Table 7-11 Configuring CPU Monitoring

Step	Command	Description
Enter the privileged mode	**enable**	-
Enable CPU occupancy monitoring of the processes.	**spy cpu**	Mandatory. By default, CPU occupancy monitoring is disabled.
Enable history statistics of CPU occupancy.	**monitor cpu**	Optional By default, history statistics of CPU occupancy is enabled.
Enter the global configuration mode	**configure terminal**	
Set the sampling cycle time of CPU occupancy statistics	**cpu sample period** *period-time*	Optional By default, the sampling time of the CPU occupancy statistics is 60s.

7.2.9. Configure Display of Properties in Pages

Configuration Condition

None

Configure Display of Properties in Pages

System information can be displayed in pages, making it easy for users to view the information. Users can set to display device information in pages according to the actual requirement.

Table 7-12 Configuring Display of Properties in Pages

Step	Command	Description
Enter the privileged mode.	**enable**	-
Configure display of properties in pages.	**more** { **on** | **off** | **help|displine** [*num*] }	Mandatory. By default, the function of display in pages is enabled. By default, 24 lines are displayed in **displine**.

7.2.10. Configure Memory Usage Alarm Threshold

Configuration Condition

None

Configure Memory Usage Alarm Threshold

The function of configuring memory usage alarm threshold can alarm when the memory usage reaches the threshold value, so that it is convenient to understand the system memory usage. The memory usage alarm threshold supports MPU configuration.

Table 7-13 Configure MPU memory usage alarm threshold

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure MPU memory usage alarm threshold	**memory utilization warner-threshold** *value*	Mandatory By default, the MPU memory usage alarm threshold is 95%.

7.2.11. Configure Low Memory Usage Threshold

Configuration Condition

None

Configure Low Memory Usage Threshold

This value is used for memory threshold processing. If the system memory is less than this value, it will enter the memory shortage state. The default value of this configuration varies with the product device. For example, for MP2900X, it is 16M.The high value of memory threshold is 50% higher than the low value. After the threshold is configured, the service module will enter the restricted operation state when the memory is short, so as to ensure the overall stability of the system.

Table 7-14 Configure low memory usage threshold

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure low memory usage threshold	**memory threshold low** *<16-500>*	Mandatory By default, the low memory using threhold is 16M.

7.2.12. System Management Monitoring and Maintaining

Table 7-15 System Management Monitoring and Maintaining

Command	Description
show clock	Display the information about the system clock.
show cpu [monitor]	Display the information about the CPU usage.
show device	Display the device information of the system.
show system environment	Display the information about the board temperature.
show history	Display the information about history commands.
show language	Display the information about system language version.
show login-secure [telnet | ssh | ftp | snmp] {ip-addr | user | quick-connect}	Display the system login information.
show mbuf allocated [*pool-name*]	Display the mbuf information.
show memory	Display the memory information.

Command	Description
show pool [**detail** | **information**]	Display the information about the memory pool.
show process [*task-name*]	Display the main tasks in the system and their operating statuses.
show semaphore { *sem-name* | **all** | **binary** | **counting** | **list** | **mutex** } [**any** | **pended** | **unpended**]	Display the information about the system semaphore.
show spy	Display the status of the monitoring switch.
show stack	Display the usage of each task stack in the system.
show system fan	Display the fan information.
show system lpu [*lpu-num* | **brief**]	Display the LPU information.
show system mpu [**brief | local | peer**]	Display the MPU information.
show system power [*power-num*]	Display the power supply information.
show tech-support all [**page | to-flash | to-memory**]	View the basic information of all moules
show tech-support L3-base [**detail** [**page**] **| page | to-flash | to-memory**]	View the basic information and detailed information of the L3 module
show tech-support sys-base [**detail** [**page**] **| page | to-flash | to-memory**]	View the basic information and detailed information of the system basic module
show version [*mpu-id* **| all**]	Display the system version information.

8. SYSTEM ALARM

8.1. Overview

With the system alarm function, if an exception occurs, the system sends an alarm prompt message so that the user can pay attention to the exception of the device and take the corresponding measures to ensure stable operation of the device. System alarms include temperature alarms, power supply abnormality alarms, and fan abnormality alarms. For the system temperature alarms, if the CPU or environment temperature reaches the threshold, generate abnormal system alarm log information and send trap (trap needs to be configured). After the power supply and fan become abnormal, also generate abnormal system alarm log information and send trap (trap needs to be configured).

8.2. System Alarm Function Configuration

Table 8-1 System Alarm Function List

Configuration Tasks	
Configure system temperature alarm switch	Configure system temperature alarm switch
Configure the system temperature alarm parameters	Configure the system temperature alarm parameters
Configure the system CPU alarm	Configure the system CPU alarm
Configure the system memory alarm	Configure the system memory alarm
Configure system fan alarms.	Configure system fan alarms.

8.2.1. Configure System Temperature Alarm Switch

Configuration Condition

Before configuring system temperature alarm switch, ensure that:

- After the system is started stably, all boards are loaded successfully.
- After the system is started stably, the power supply and fans operate normally.

Configure System Temperature Alarm Switch

Configuring the system temperature alarm refers to whether the system alarm log information will be generated and the related trap will be sent when the temperature alarm log is generated (trap needs to be configured).

Table 8-2 Configure the system temperature alarm switch

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the system temperature alarm switch	**[no] alarm { temperature } enable**	Mandatory When the switch is disabled, the alarm temperature log will not be printed. By default, it is enabled.

8.2.2. Configure System Temperature Alarm Parameters

Configuration Condition

Before configuring system alarms, ensure that:

- After the system is started and operates stably, all boards are loaded successfully.
- After the system is started and operates stably, the power supply and fans operate normally.

Configure System Temperature Alarms

Configuring the system temperature alarm means that when the temperature of the MPU reaches a certain threshold, the system alarm log information will be generated and the related trap will be sent (trap needs to be configured).

Table 8-3 Configuring System Temperature Alarms

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the system temperature alarm switch	**[no] alarm temperature enable**	Mandatory When the switch is disabled, the temperature alarm log will not be printed. By default, it is enabled.
Configure the system temperature alarm threshold	**[no] alarm temperature** { mpu } **{ cpu | switch-chip}** *temperature-value*	Mandatory.

8.2.3. Configure System CPU Alarm

Configuration Condition

Before configuring the system alarm, first complete the following task:

- After the system is started and operates stably, all boards are loaded successfully.

Configure System CPU Alarm

Configuring the system CPU alarm indicates that after configuring the CPU utilization monitor threshold, generate the CPU utilization abnormal alarm when exceeding the monitor threshold.

Table 8-4 Configure the system CPU alarm

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the system CPU utilization alarm threshold	**cpu utilization warner-threashold** [*rate-value*]	Optional By default, it is not enabled.

8.2.4. Configure System Memory Alarm

Configuration Condition

Before configuring the system alarm, first complete the following task:

- After the system is started and operates stably, all boards are loaded successfully.

Configure System Memory Alarm

Configuring the system memory alarm indicates that after configuring the system memory utilization monitor threshold, generate the system memory utilization abnormal alarm when exceeding the monitor threshold.

Table 8-5 Configure the system memory alarm

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the system memory utilization alarm threshold	**memory utilization warner-threashold** [*rate-value*]	Optional By default, the system memory utilization alarm threshold is 95%.

8.2.5. Configure System Fan Alarms

Configuration Condition

None

Configure System Fan Alarms

If a system fan fault or exception occurs, the system immediately generates log information about the system fan alarm. This helps the user to pay attention to the exception of the device fans and take the corresponding measures to get rid of the fault and ensure stable operation of the device. By default, the system fan alarm function is enabled.

9. SYSTEM LOG CONFIGURATION

9.1. Overview

The log information is categorized into eight levels, including: **emergencies**, **alerts**, **critical**, **errors**, **warnings**, **notifications**, **informational**, and **debugging**. Here levels 0-6 are log information and level 2 is debugging information. For details, refer to the following table.

Table 9-1 Description of the System Log Level Fields

Field	Level	Description
emergencies	0	Fatal fault. The system is unavailable, the device stops and it needs to be restarted.
alerts	1	Serious error. Functions of a certain type become unavailable, and the services are stopped.
critical	2	Critical error. Irreversible problems occur on the functions of a certain type, and some functions are affected.
errors	3	Error message.
warnings	4	Warning message.
notifications	5	Event notification message.
informational	6	Message prompt and notification.
debugging	7	Debugging message.

The log information is outputted to five directions: control console (Console terminal), monitor console (Telnet or SSH terminal), log server, log files (memory log files and flash log files), and email. The output to the five directly is controlled by respective configuration commands. The debugging information is outputted to two directions, control console and monitor console. The log information can also be configured to output to the log server or log files.

Table 9-2 Log Output Directions

Log Output Direction	Description
Control console	The log information is outputted to the Console terminal.
Monitor console	The log information is outputted to the Telnet or SSH terminal.
Log server	The log information is outputted to the log server. By default, logs of levels 0-5 are outputted to the log server.
Log files	The log information is outputted to the system memory or flash memory. By default, log information of levels 0-5 is outputted to the system memory, and log information of levels 0-5 is outputted to the flash memory.
email	The log information is output to the email. By default, the logs of levels 0-4 are outputted to the log email.

The log module runs in a separate syslog process. The main thread of the syslog process receives the log information sent by the system. Firstly, process the log data and distribute the cache space. Then, load the configured output actions to the corresponding buffer queue of each output terminal. Because of the length limitation of the cache queue, when a large number of log information is output, there is a loss of log information. At this time, the log module will count the lost messages. There are two threads in the output of log scheduling (when the log information is output to the console, monitor, log server, run in the same sub-thread as log files; when the log information is output to email, run in another sub-thread). In the scheduling thread, enable a timer for each output direction, and after responding each time, the timer gets the log information data from the queue corresponding to the terminal and outputs to the corresponding terminal according to the user configuration.

9.2. System Log Function Configuration

Table 9-3 System Log Function List

Configuration Tasks	
Configure log output functions	Configure log output to the control console.
	Configure log output to the monitor console.
	Configure log output to the server.
	Configure log output to files.
	Configure log output to email
Configure the timestamp for logs.	Configure the timestamp for logs.
Configure the operation log to be sent to the log server	Configure the operation log to be sent to the log server
Configure the log repeat suppression function	Configure the log repeat suppression function
Configure the log file capacity.	Configure the log file capacity.
Configure the log file encryption function	Configure the log file encryption function
Configure log display colors.	Configure log display colors.

9.2.1. Configure Log Output Functions

Configuration Condition

None

Configure Log Output to the Control Console

The control console refers to a Console terminal. It is a channel through which the system output log information to the control console.

Table 9-4 Configuring Log Output to the Control Console

Step	**Command**	**Description**
Enter the global configuration mode.	**configure terminal**	-
Enable the log output function.	**logging enable**	Optional. By default, the log output function is enabled.
Enable log display on the control console.	**logging source** { *module-name* | **default** } **console** { **level** *severity* | **deny** }	Optional. By default, log display on the control console is enabled.

Configure Log Output to the Monitor Console

The monitor console refers to the Telnet or SSH terminal. It is used for remote device management. To configure the log output to the monitor console, you need to enable the log display on the current terminal.

Table 9-5 Configuring Log Output to the Monitor Console

Step	**Command**	**Description**
Enter the global configuration mode.	**configure terminal**	-
Enable the log output function.	**logging enable**	Optional. By default, the log output function is enabled.
Enable log display on the monitor console.	**logging source** { *module-name* | **default** } **monitor** { **level** *severity* | **deny** }	Optional. By default, the log display function of the global monitor console is enabled.
Enable log display of the current monitor console.	**terminal monitor**	Mandatory. By default, log display on the current monitor console is disabled.

Configure Log Output to the Server

To record the log information in a more comprehensive manner, you can configure the log information output to the log server, which is convenient for the maintenance and management of the system. When configuring the log output to the log server, you need to configure the host address or domain name of the log server.

Table 9-6 Configuring Log Output to the Log Server

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the log output function.	**logging enable**	Optional. By default, the log output function is enabled.
Configure the log output to the log server	**logging server** *server-name* [**vrf** *vrf-name*] { **ip** *ip-address* | **ipv6** *ipv6-address* | **hostname** *host-name*} [**port** *port-num*] [**facility** *facility-name*] **[level** *severity***]**	Mandatory By default, do not configure the log output to the log server.
Configure the IP source address for sending the log information	**logging server source** { **ip** *ip-address* | **ipv6** *ipv6-address* | **interface** *interface-name* }	Optional By default, confirm the output interface of sending the log information by the route, and use the master IP address of the output interface as the source IP address of the sent log information.
Configure the log information of the specified level output to the log server	**logging source** { *module-name* | **default** } **server** [*server-name &<1-8>*] { **level** *severity* | **deny** }	Optional By default, the log information of level 0-5 can be output to the log host.

Configure Log Output to Files

Log files can be stored in two manners, in the memory, and in the flash memory. The memory stores only the log information from device syslog startup to the system restarting or before syslog process restarting. By default, log information of level 5 (notifications) and higher levels are stored. By default, the flash memory stores log information of level 5 (**notifications**) and higher levels. For the levels of logs, refer to the detailed description in Table 9-1. Both the two types of log files have capacity limit. If the size of log files reaches the configured maximum capacity, first delete the oldest log file (the log information is recorded by multiple log files) when adding one log, and then, add one log file and record the log information to the new log file.

Table 9-7 Configuring Log Output to Files

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the log output function.	**logging enable**	Optional. By default, the log output function is enabled.
Configure the log output to Flash	**logging source** { *module-name* | **default** } **file** { **level** *severity* | **deny** }	Optional By default, the log information of level 0-5 is saved to Flash.
Configure the log output to memory	**logging source** { *module-name* | **default** } **buffer** { **level** *severity* | **deny** }	Optional By default, the log information of level 0-5 is saved to memory.
Configure the log file capacity alarm	**logging** { **buffer** | **file** } **warning** *warning-value recover-value*	Optional By default, the log information warning value is 90%, and the recover value is 70%.
Configure the log file compression	**logging compress [gunzip]** **logging compress max-num** *value*	Optional By default, do not enable the log compression function.

Configure Log Output to Email

In order to record the log information more comprehensively, we can configure the log information to be output to the email box of the recipient and copier through email.

Table 9-8 Configuring Log Output to Email

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the log output function.	**logging enable**	Optional. By default, the log output function is enabled.
Configure the email profile	**logging email** *email-profile*	Mandatory By default, do not configure the profile of outputting the log to email.
Configure the email address of the recipient of the log information	**mail recipient** mail-address	Mandatory By default, do not configure the email address of the recipient of the log information.
Configure the email address of the copier for receiving the log information	**mail copyto** mail-address	Optional By default, do not configure the email address of the copier for receiving the log information.
Configure the email address of the sender of the log information	**mail sender** *mail-address*	Mandatory By default, do not configure the email address of the sender of the log information.
Configure the email password of the sender of the log information	**mail sender password** *{0 plain-key | 7 cipher-key}*	Mandatory By default, do not configure the email password of the sender of the log information. 0 means to configure plaintext password, 7 means to configure ciphertext password, and ciphertext password is generated by configuring plaintext password.

Step	Command	Description
Configure the email domain name address of the receiver of the log information	**mail server** *server-name*	Optional By default, take the characters after the @ in the email address of the sender as the domain name address of the sender.
Configure the email subject of sending the log information	**mail subject** *subject-name*	Optional By default, do not configure the email subject of sending the log information.
Configure the log information of the specified level output to the email box of the receiver and copier via email	**logging source** { *module-name* | **default** } **email** { **level** *severity* | **deny** }	Optional By default, the log information of level 0-4 is output to email.

9.2.2. Configure the Timestamp for Logs

Configuration Condition

None

Configure the Timestamp for Logs

The timestamp of a log records in details the time at which the log is generated. By default, log timestamps adopt the absolute time format, but they also support Uptime (relative time) format. The absolute time format records the year and the time with millisecond precision. It outputs the time of logs in details.

Table 9–9 Configuring the Timestamp for Logs

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the timestamp type of the log information	**logging timestamps uptime**	Optional By default, the log information adopt the absolute stamp type.

Step	Command	Description
Configure the timestamp format for logs.	**logging timestamp-format { msec | timezone | year }**	Optional By default, the log information adopts the timestamp format with the year to display.

Note:

- The uptime refers to the run time starting with device startup.
- The datetime refers to the time of the real-time clock.
- The localtime refers to local time

9.2.3. Configure Operation Log Output to Log Host

Configuration Condition

You need to configure the log output to the host first.

Configure Operation Log Output to Log Server

After configuring the operation log output to the log server, you can query the operation log of the user on the log server.

Table 9–10 Configure the operation log output to the log host

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the log output function	**logging enable**	Optional By default, the log output function is enabled.
Configure the log host	**logging server** *server-name* [**vrf** *vrf-name*] { **ip** *ip-address* | **ipv6** *ipv6-address* | **hostname** *host-name* } [**port** *port-num*] [**facility** *facility-name*] **[level** *severity***]**	Mandatory By default, the function of sending the log information to the log server is not enabled.
Configure the operation log sent to the log server	**logging operation to-server**	Mandatory By default, the function of sending the operation log to the log server is not enabled.

9.2.4. Configure Log Repeat Suppression

Configuration Condition

None

Configure Log Repeat Information Suppression

In some cases, the module may continuously output the same log, affecting the observation of other logs. At this time, you can enable the repeat suppression function the log information. The repeated log information is output once in each suppression period, and the times that the log is suppressed in the suppression period is output at the end of the suppression period.

Table 9–11 Configure the log repeat suppression

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the suppression function of the log repeat information	**logging suppress duplicates interval** *interval-num*	Mandatory By default, the log suppression function is enabled.

9.2.5. Configure the Log File Capacity

Configuration Condition

None

Configure the Log File Capacity

Limited by the capacity of the flash memory, the log file capacity can be configured from 1M-32M bytes. When the size of stored log information exceeds the maximum capacity limit, the new log overwrites the old log information (take the file as the unit to cover the old log information file).

Table 9-12 Configuring the Log File Capacity

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the log file capacity.	**logging file size** *file-max-size*	Optional. By default, the log file capacity is 1M bytes.

9.2.6. Configure Log File Encryption

Configuration Condition

None

Configure Log File Capacity

Considering the security of log information, the log files stored in flash can be encrypted. When configuring the encryption function of log files, the subsequent generated logs will be stored in the log file as ciphertext. If the password of log files changes, the previously stored logs in ciphertext will not be displayed in plaintext. The log information be stored in the form of plaintext only when the password is reconfigured as the password when the log is generated.

Table 9-13 Configure Log File Encryption

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the log file encryption	***logging file encryption alogrithms SMV4 key*** {0 plain-key | 7 cipher-key}	Optional By default, do not configure the encryption function for the log file in Flash. 0 means to configure plaintext password, 7 means to configure ciphertext password, and ciphertext password is generated by configuring plaintext password

9.2.7. Configure Log Display Colors

Configuration Condition

None

Configure Log Display Colors

When log information is displayed, you can modify log information of different levels so that they are displayed in different colors. In this way, the importance degrees of logs are distinguished. By default, the log display color function is enabled. The following table shows the default colors corresponding to the log levels.

Table 9-14 Description of Log Colors

Field	Description
emergencies	Red
alerts	Purple
alerts	Blue
errors	Brown
warnings	Cyan
notifications	White
informational	Green
debugging	Green

Table 9-15 Configuring Log Display Colors

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure a color for logs of a level.	**logging color** [*logging-level logging-color*]	Optional. By default, each log level has a corresponding log display color.

Note:

- If the control console or monitor console needs to output log information in different colors, you need to configure the color option of the terminals; otherwise, no color is displayed for the log information.

9.2.8. Configure Log Filtering Function

Configuration Condition

None

Configure Log Filtering Function

When configuring the log filtering, you can not only specify displaying the log information with the filtering character string, but also can display the log information and log information level range without the filtering character string. When using the command, the filtering character string needs to be used with the log level range.

Table 9–16 Configure the log filtering function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the log filtering function	**logging filter** { **exclude** *exclude-string* | **include** *include-string* | **level** *high-level low-level* }	Optional By default, the log filtering function is not enabled.

9.2.9. Log Monitoring and Maintaining

Table 9-17 Log Monitoring and Maintaining

Command	Description
clear logging [**buffer** | **file**]	Clear the log information stored in memory or Flash
show logging [**buffer** | **file**]	Display the log information that is stored in the memory or flash memory.
show logging { **file** | **buffer** } **desc**	Reversely display the log information stored in the memory or Flash
show logging filter	Display the filtering configuration information of the log
show logging operation	Display the log information stored in the operation log file
show logging [{ **file** | **buffer** } [**begin-level** *level-value* **/** [**start-time** *stime* [**end-time** *etime*]] [**detail**]]]	Display the log information stored in log files, filtering to display the log information with the time and level filtering option
show logging { file | buffer } message-counter	Display the size of the log file and the number of the log information entries stored in Flash or memory.

10. SOFTWARE UPGRADE

10.1. Overview

Software upgrade provides a more stable software version and more abundant software features for the user.

Upgraded programs are stored in the storage mediums of the device in the form of files or data blocks. The software modules with different functions cooperate to keep the device in the stable working state and support the hardware features of the device and application services of users.

Users can upgrade software through the TFTP/FTP network transmission mode or the Xmodem transmission mode of the Console port. In upgrading software of different types, users must carefully read the operation steps and notes and cautions described in the manuals related to the software upgrade.

In upgrading software, you usually need to upgrade software of each type. If the software of a type is not updated during the upgrade process, you need not upgrade the software again. Usually, you can restart the device only after the all software versions are upgraded.

The following types of software are available:

- The image program package: The program package of the main board with the suffix pck. It contains a group of programs that are required for normal operation of the system, including operating system and application programs.
- **FPGA** (**Field Programmade Gate Array**) program: the program with suffix bin, which is mainly used to realize the logic control of devices and the sending and receiving of service data.
- The Bootloader program: The program with the suffix .bin or. pck, the boatloader program of the main control board, fixed in the ROM of the main control board and the main board of the business board, is executed first after the device is powered on. This program initializes the basic system, and its main function is to guide the operating system to load.
- **CPLD(Complex Programmable Logic Device) program**: The program with the suffix .pck, the digital integrated circuit for constructing the logic function
- **Devinfo**: OEM program, including model ID and function ID of various devices and boards. It is mainly used for upgrading when the device is modified.
- **Package program**: The package file with the image, Bootloader, cmm, devinfo program, which can upgrade various types of software programs once.

The applicable relationship between the above types of upgrade software and each type of board card is shown in the table:

Table 10-1 Applicable relationship between upgrade programs and boards

	Image program package	fpga program	bootload program	cpld program	devinfo file	package file
Main control board	√	√	√	√	√	√
Service board subcard	-	√	-	-	-	-

Note:

- POS and other WAN service cards have FPGA program, but Ethernet service board sub card has no FPGA program.

10.2. Software Upgrade Function Configuration

Table 10-2 Software Upgrade Function List

Configuration Tasks	
Upgrade the image program package.	Upgrade the image program package of the main control board in TFTP/FTP mode.
Upgrade the FPGA program	Upgrade the FPGA program via the TFTP/FTP mode
Upgrade the Bootloader program.	Upgrade the Bootloader program in TFTP/FTP mode.
Upgrade the cpld program	Upgrade the cpld program in the TFTP/FTP mode
Upgrade the devinfo file	Upgrade the devinfo file package in TFTP/FTP mode.
Upgrade the package program.	Upgrade the package program via the TFTP/FTP mode

10.2.1. Upgrade the image Program Package

The image program package is used to upgrade the main control board.

Configuration Preparations

Before upgrading the image program package, ensure that:

- The route between the TFTP/FTP server and the device interface is reachable, and the TFTP/FTP server and the device can ping each other successfully.
- The TFTP/FTP server configuration is correct, and the image program is stored in the specified directory of the TFTP/FTP server.
- The remaining space of the flash is sufficient. If the space is insufficient, manually delete the unnecessary files in the flash.
- The configuration files have been backed up.

Upgrade the image Program Package in TFTP/FTP Mode

Enter the privileged user mode, ensure that the device can obtain the upgrade program through the external TFTP/FTP server, and then use the **sysupdate image** command to upgrade the program package.

Table 10-3 Upgrading the image Program Package in TFTP/FTP Mode

Step	Command	Description
Enter the privileged user mode.	None	Mandatory.
Upgrade the image program package.	**sysupdate image mpu** [**vrf** *vrf-name*] {*dest-ip-address* **|** *dest-ipv6-address*} *filename* [**ftp** *ftp-username ftp-password*] [**reload**]	Mandatory. If the FTP option is not specified, TFTP is used for upgrade by default.

Example: In the standalone mode, make use of the FTP server 130.255.168.45 to upgrade the image program package of the online main control board.

```
Hostname#sysupdate image mpu 130.255.168.45 rp34-7.7.0.106(R).pck ftp a a
```

#The device gives the following prompt messages:

```
checking "rp34-7.7.0.106(R).pck" : ...OK

downloading "rp34-7.7.0.106(R).pck" :
######################################################################
#OK

Download "rp34-7.7.0.106(R).pck" (71143624 Bytes) successfully.

Verify the image...

Apr  7 2020 10:41:25 router MPU0 %SYS_UPDATE-RESULT-5:image : Mpu 0 download file
successfully!valid

Writing file to filesystem.............................................................................OK!
```

```
Start backup ios to raw flash...
Apr  7 2020 10:41:56 router MPU0 %SYS_UPDATE-RESULT-5:image : Mpu 0 write file to file-
system successfully!OK
 %Sysupdate image is in process, please wait...
Apr  7 2020 10:42:54 router MPU0 %SYS_UPDATE-RESULT-5:image : Mpu 0 write file to backup
file-system successfully!
Apr  7 2020 10:42:54 router MPU0 %SYS_UPDATE-RESULT-5:image : Mpu 0 upgrade
successfully!
 %Sysupdate image finished.


      sysupdate image result information list:
------------------------------------------------------------
      Card      result information
------------------------------------------------------------
      Mpu 0      upgrade successfully!
```

#The above message indicates that the image program of the active control cards has been upgraded successfully.

Note:

- If the command option reload is added, the system prompts whether to save the configuration and whether to restart the device. Usually, the device is started after all programs are upgraded. Therefore, the reload option is not recommended.
- Before the upgrade, ensure that there is sufficient remaining space in the flash. If the space is insufficient, the upgrade fails. In this case, you can manually delete files that are not in need from the flash to obtain more space for upgrading application programs.
- When the flash space of the control card is insufficient, it will prompt whether to delete the redundant image files. If the space is still insufficient after deleting, the upgrade fails.
- It takes a long time to upgrade the image program package. A smaller remaining space in the flash results in longer upgrade time.
- After the upgrade is completed, to run the new image program, restart the device.
- If the device fails to start normally, open the Bootloader screen, modify the startup mode to network startup. After the device is started successfully, start the upgrade. For the method, refer to the related section in the Bootloader configuration manual and command manual.

Router supports IPv6 upgrade; Using IPv6 upgrade to ensure that the ftp/tftp used supports IPv6 services.

Warning:

- During the upgrade process, you cannot power off the device or swap or restart the main control board. Otherwise, the system may fail to start, or the flash file system of the main control board may be damaged.

10.2.2. Upgrade the fpga Program

The FPGA program is used to upgrade the service card.

Configuration Preparations

Before upgrading the FPGA program, ensure that:

- The route between the TFTP/FTP server and the device interface is reachable, and the TFTP/FTP server and the device can ping each other successfully.
- The TFTP/FTP server configuration is correct, and the FPGA program is stored in the specified directory of the TFTP/FTP server.
- Back up the configuration files.

Upgrade the FPGA Program via TFTP/FTP

Enter the privileged user mode, ensure that the device can obtain the upgrade program through the external TFTP/FTP server, and then use the **sysupdate fpga** command to upgrade the program package.

Table 10-4 Upgrade the FPGA program via TFTP/FTP

Step	Command	Description
Enter the privileged user mode.	None	Mandatory.
Upgrade the FPGA program	**sysupdate fpga mpu | lpu | all }{** *cardNo* **| all }} | all** } [**vrf** *vrf-name*] {*dest-ip-address* **|** *dest-ipv6-address*} *filename* [**ftp** *ftp-username ftp-password*] [**reload**]	Mandatory If the FTP option is not specified, use the TFTP to upgrade by default.

Example: Upgrade the FPGA program of the service card via the FTP server 130.255.168.45 automatically.

```
Hostname#sysupdate fpga lpu all 130.255.168.45 ir0094ce1_fp_lx16_v003_103.bin ftp a a
```

#The device will prompt the following information:

```
checking "ir0094ce1_fp_lx16_v003_103.bin" : ...OK
downloading "ir0094ce1_fp_lx16_v003_103.bin" : #OK
Download "ir0094ce1_fp_lx16_v003_103.bin" (464324 Bytes) successfully.
Update FPGA of LPU1: ......................................................Successfully! image verify ...................................................................................OK

 %Sysupdate fpga is in process, please wait...
 %Sysupdate fpga finished.
        sysupdate fpga result information list:
--------------------------------------------------------------
        Card       result information
--------------------------------------------------------------
```

```
    Lpu 1      upgrade successfully!
```

#The above information indicates that the FPGA program of the service card is upgraded successfully.

Note:

- When upgrading FPGA, if the board type is not specified, the corresponding board will be automatically searched according to the FPGA program type for upgrading.
- After the upgrade, if you need to run a new FPGA program, you need to restart the board or the whole device.
- The router supports IPv6 upgrade; When upgrading with IPv6, ensure that FTP/TFTP supports IPv6 service.

Warning:

- In the process of upgrading, the device cannot be powered off, and it is forbidden to plug or restart the board. Otherwise, the system may fail to start and the FPGA file of the board may be damaged.

10.2.3. Upgrade the Bootloader Program

The Bootloader program is used to upgrade the main control card.

Configuration Preparations

Before upgrading the Bootloader program, ensure that:

- The route between the TFTP/FTP server and the device interface is reachable, and the TFTP/FTP server and the device can ping each other successfully.
- The TFTP/FTP server configuration is correct, and the Bootloader program is stored in the specified directory of the TFTP/FTP server.

Upgrade the Bootloader Program in TFTP/FTP Mode

Enter the privileged user mode, ensure that the device can obtain the upgrade program through the external TFTP/FTP server, and then use the **sysupdate Bootloader** command to upgrade the program package.

Table 10-5 Upgrading the Bootloader Program in TFTP/FTP Mode

Step	Command	Description
Enter the privileged user mode.	None	Mandatory.
Upgrade the Bootloader program.	**sysupdate Bootloader mpu** [**vrf** *vrf-name*] {*dest-ip-address* **|** *dest-ipv6-address*} *filename* [**ftp** *ftp-username ftp-password*] [**reload**]	Mandatory. If the FTP option is not specified, TFTP is used for upgrade by default.

Example:

Make use of FTP server 130.255.168.45 to upgrade the Bootloader program of the online main control board.

```
Hostname#sysupdate Bootloader mpu 130.255.168.45 rp34-Bootloader-b2-1.0.0.01.pck ftp a a
```

#The device will prompt the following information:

```
checking "rp34-Bootloader-b2-1.0.0.01.pck" : ...OK
downloading "rp34-Bootloader-b2-1.0.0.01.pck" : ##OK
Download "rp34-Bootloader-b2-1.0.0.01.pck" (1644852 Bytes) successfully.
Update Bootloader start.


Apr  7 2020 11:12:27 router MPU0 %SYS_UPDATE-RESULT-5:Bootloader : Mpu 0 download file successfully!................................OK.


 %Sysupdate Bootloader is in process, please wait...
Apr  7 2020 11:12:55 router MPU0 %SYS_UPDATE-RESULT-5:Bootloader : Mpu 0 upgrade successfully!
 %Sysupdate Bootloader finished.


      sysupdate Bootloader result information list:
--------------------------------------------------------------
      Card       result information
--------------------------------------------------------------
      Mpu 0      upgrade successfully!
```

#The above message indicates that the Bootloader program of the online main control card has been upgraded successfully.

Note:

- When upgrading, please select the correct version of Bootloader and upgrade the Bootloader of all service cards on the device synchronously to avoid abnormal situation.
- If the command option reload is added, the system prompts whether to save the configuration, and whether to restart the device immediately. However, usually the device is started after all programs are upgraded. Therefore, the reload option is not recommended. Please select the correct version of Bootloader for upgrading to avoid exception.
- The router supports IPv6 upgrade; When upgrading with IPv6, ensure that FTP/TFTP supports IPv6 service.

Warning:

- During the upgrade process, you cannot power off the device or swap or restart the main control board and service card. Otherwise, the system may fail to start, or the Bootloader file of the board card may be damaged.

Upgrade the Bootloader Program via the Console Port

Ensure that the HyperTerminal can access the device through the Console port. Enter the Bootloader mode, adjust the baud rate, and perform the upgrade through the ymodem of the HyperTerminal. If there are two master cards on the device, you need to upgrade them separately.

For details of the commands, refer to the related chapter of the “Bootloader” command manual.

Table 10-6 Upgrading the Bootloader Program via the Console Port

Step	Command	Description
Set the HyperTerminal.	None	Mandatory. Run the HyperTerminal program, select the corresponding serial port (such as com1) and set its properties. Set baud rate to 9600 bps, soft flow control, 8 data bits, no parity check, and 1 stop bit.
Enter the Bootloader mode.	None	Mandatory. When the device restarts, press Ctrl + C to enter the Bootloader mode.
Modify the baud rate of the Console port and HyperTerminal to improve the upgrade speed.	**srate** { *speed* }	Optional. Modify the baud rate of the device Console port to 115200 bps. Then, disconnect the HyperTerminal, and modify the baud rate of the HyperTerminal to 115200 bps, and then connect the HyperTerminal again.
Upgrade the Bootloader program.	**mupdate Bootloader**	Mandatory. In the Bootloader mode, input the mupdate Bootloader command, select the ymodem protocol of the HyperTerminal, and select the Bootloader program to start transmission.

Example:

The following example shows how to upgrade the Bootloader program of the control card through the Console port.

#The device gives the following prompt messages:

```
Bootloader# mupdate Bootloader
Download Bootloader start...
run command=loady
## Ready for binary (ymodem) download to 0x20000000 at 9600 bps...
CC
Starting xmodem transfer.  Press Ctrl+C to cancel.
Transferring rp34-Bootloader-b2-1.0.0.01.pck...
  100%    1740 KB      3 KB/sec    00:07:28       3 Errors

xyzModem - CRC mode, 13923(SOH)/1(STX)/0(CAN) packets, 6 retries
## Total Size      = 0x001b3168 = 1782120 Bytes
Download Bootloader OK.
Bootloader image check:
Image validated. Header size 192, data size 1781928
                Header crc 0x5df446ee, data crc 0xf2a652f8
                Image link address is 0xffffffffc0000000
....................................... done
Un-Protected 39 sectors

....................................... done
Erased 39 sectors
run command=cp.b $(loadaddr) 0x1f400000 0x200000
Copy to Flash... done
....................................... done
Protected 39 sectors
Update Bootloader OK.
Bootloader#
```

#The above message indicates that the Bootloader program of the control card has been upgraded successfully.

Note:

- In upgrading the Bootloader program, ensure that the rate of the HyperTerminal is the same as the rate of the device Console port.
- In upgrading the Bootloader program, the transmission speed is recommended to be set to 115200 bps. In this way, the upgrade transmission time is shorter.

- If the default rate of the Console port has been modified in upgrading the Bootloader program, in loading the image program package, the rate of the device Console port automatically resumes to 9600bps. At this time, the rate of the HyperTerminal needs to be modified synchronously.
- It is recommended that you upgrade the Bootloader program in TFTP/FTP mode. The Console port upgrade mode is used only when the upgrade conditions of the first upgrade mode fail to be satisfied.
- When using IPv6 to upgrade, ensure that the used FTP/TFTP supports the IPv6 service.

Warning:

- During the upgrade process, you cannot power off the device or swap or restart the main control board. Otherwise, the system may fail to start, or the Bootloader file of the board card may be damaged.

10.2.4. Upgrade the cpld Program

The CPLD file is used to upgrade the control card, forwarding card, service board mother card and service board daughter card.

Configuration Preparations

Before upgrading the CPLD file, ensure that:

- The route between the TFTP/FTP server and the device interface is reachable, and the TFTP/FTP server and the device can ping each other successfully.
- The TFTP/FTP server configuration is correct, and the CPLD file is correctly stored in the specified directory of the T2FTP/FTP server.
- Back up the configuration file.

Upgrade the CPLD File in TFTP/FTP Mode

Enter the privileged user mode, ensure that the device can obtain the upgrade program through the external TFTP/FTP server, and then, use the **sysupdate CPLD** command to upgrade the program package.

Table 10-7 Upgrade the CPLD file in the TFTP/FTP mode

Step	Command	Description
Enter the privileged user mode.	None	Mandatory.
Upgrade the CPLD file	**sysupdate cpld mpu** [**vrf** *vrf-name*] {*dest-ip-address* **|** *dest-ipv6-address*} *filename* [**ftp** *ftp-username ftp-password*] [**reload**]	Mandatory If not specifying the FTP option, use TFTP to upgrade by default.

Example:

Make use of FTP server 130.255.168.45 to upgrade the cpld program of the online control boards.

```
Hostname#sysupdate cpld mpu 130.255.168.45 pr019_cpld_RM7E_clv007.pck ftp a a
```

#The device will prompt the following information:

```
checking "pr019_cpld_RM7E_clv007.pck" : ...OK
downloading "pr019_cpld_RM7E_clv007.pck" : #OK
Download "pr019_cpld_RM7E_clv007.pck" (423584 Bytes) successfully.
 %Sysupdate cpld is in process, please wait...
 %Sysupdate cpld finished.

        sysupdate cpld result information list:
--------------------------------------------------------------
        Card       result information
--------------------------------------------------------------
        Mpu 0      upgrade successfully!
```

#The above information indicates that the CPLD file of the online card is upgraded successfully.

Note:

- After upgrading CPLD, you need to power off and restart the device.
- The router supports IPv6 upgrade; When upgrading with IPv6, ensure that FTP/TFTP supports IPv6 service.

Warning:

- During the upgrade process, you cannot power off the device or swap or restart the main control board. Otherwise, the system may fail to start, or the CPLD file may be damaged.

10.2.5. Upgrade the devinfo File

The devinfo file is used to upgrade the main control board.

Configuration Preparations

Before upgrading the devinfo file, ensure that:

- The route between the TFTP/FTP server and the device interface is reachable, and the TFTP/FTP server and the device can ping each other successfully.
- The TFTP/FTP server configuration is correct, and the devinfo file is stored in the specified directory of the TFTP/FTP server.
- Back up the configuration file.

Upgrade the devinfo File in TFTP/FTP Mode

Enter the privileged user mode, ensure that the device can obtain the upgrade program through the external TFTP/FTP server, and then use the sysupdate devinfo command to upgrade.

Table 10-8 Upgrading the devinfo File in TFTP/FTP Mode

Step	Command	Description
Enter the privileged user mode.	None	Mandatory.
Upgrade the devinfo file	**sysupdate devinfo mpu** [**vrf** *vrf-name*] {*dest-ip-address* **|** *dest-ipv6-address*} *filename* [**ftp** *ftp-username* *ftp-password*] [**reload**]	Mandatory If the FTP option is not specified, TFTP is used for upgrade by default.

Example:

Make use of FTP server 130.255.168.45 to upgrade the devinfo file of the online main control board.

```
Hostname#sysupdate devinfo mpu 130.255.168.45 devInfo(v4.4) ftp a a
```

#The device gives the following prompt messages:

```
checking "devInfo(v4.4)" : ...OK
downloading "devInfo(v4.4)" : #OK
Download "devInfo(v4.4)" (6275 Bytes) successfully.
Writing file to filesystem....OK!

 %Sysupdate devinfo is in process, please wait...
 %Sysupdate devinfo finished.

       sysupdate devinfo result information list:
------------------------------------------------------------------
       Card      result information
------------------------------------------------------------------
       Mpu 0      upgrade successfully!
```

#The above message indicates that the devinfo file of the online main control card has been upgraded successfully.

Note:

- If the command option reload is added, the system prompts whether to save the configuration and whether to restart the device. Usually, the device is started after all programs are upgraded. Therefore, the reload option is not recommended.
- After the upgrade is completed, to run the new devinfo file, restart the device.
- The devinfo files of all cards on the device need to be upgraded synchronously to avoid exception.

- Select the correct devinfo file version to upgrade to avoid exceptions.
- The router supports IPv6 upgrade; When upgrading with IPv6, ensure that FTP/TFTP supports IPv6 service.

Warning:

- During the upgrade process, you cannot power off the device or swap or restart the main control board. Otherwise, the system may fail to start, or the devinfo file may be damaged.

10.2.6. Upgrade the Package File

The package file contains the image, Bootloader, and devinfo files, which can be upgraded once via the package file.

Configuration Preparations

Before upgrading the package file, you need to complete the following task:

- Ensure that the route between the TFTP/FTP server and the device interface is reachable, and they can ping each other.
- The TFTP/FTP server is configured correctly, and the package file is correctly placed in the specified directory of TFTP/FTP.
- Back up the configuration file.

Upgrade Package File via TFTP/FTP

Enter the privileged user mode, ensure that the device can get the upgrade program from the external TFTP/FTP server, and then, upgrade via the **sysupdate package** command.

Table 10-9 Upgrade the package file via TFTP/FTP

Step	Command	Description
Enter the privileged user mode.	None	Mandatory.
Upgrade the package file	**sysupdate package [vrf** *vrf-name*] {*dest-ip-address* **|** *dest-ipv6-address*} *filename* [**ftp** *ftp-username ftp-password* **] [no-comparision]** **[reload]**	Mandatory If not specifying the FTP option, use TFTP to upgrade by default.

Example:

Make use of FTP server 130.255.168.45 to upgrade the programs of all types of online boards in package.

```
Hostname#sysupdate package 130.255.168.45 rp34-7.7.0.106(R)-001.pkg FTP a a
```

#The device will prompt the following information:

```
Downloading "rp34-7.7.0.106(R)-001.pkg" header…OK!
```

```
Checking "rp34-7.7.0.106(R)-001.pkg" header...OK!


        image file version comparision:
-------------------------------------------------------------
Component         Component version      File version
-------------------------------------------------------------
Mpu 0             7.7.0.103(integrity)    7.7.0.106(R)
The software version of the file to be upgraded is the same or newer as the currently used version.


Downloading "rp34-7.7.0.106(R)-001.pkg" : ################################################################OK!
Download "rp34-7.7.0.106(R)-001.pkg" (64631936 Bytes) successfully!
Checking package file...OK!
Verify the image...valid
Writing file to filesystem...........................................................................................................................................................................OK!
Start backup ios to raw flash...
Apr  7 2020 09:22:52 router MPU0 %SYS_UPDATE-RESULT-5:image : Mpu 0 write file to file-system successfully!OK
 %Sysupdate image is in process, please wait...
Apr  7 2020 09:23:54 router MPU0 %SYS_UPDATE-RESULT-5:image : Mpu 0 write file to backup file-system successfully!
Apr  7 2020 09:23:54 router MPU0 %SYS_UPDATE-RESULT-5:image : Mpu 0 upgrade successfully!
 %Sysupdate image finished.
Update Bootloader start.
..............................OK.


 %Sysupdate Bootloader is in process, please wait...
Apr  7 2020 09:24:24 router MPU0 %SYS_UPDATE-RESULT-5:Bootloader : Mpu 0 upgrade successfully!
 %Sysupdate Bootloader finished.
Writing file to filesystem....OK!


 %Sysupdate devinfo is in process, please wait...
Apr  7 2020 09:24:25 router MPU0 %SYS_UPDATE-RESULT-5:devinfo : Mpu 0 upgrade successfully!
 %Sysupdate devinfo finished..
 %Sysupdate pkgInfo is in process, please wait...
Apr  7 2020 09:24:26 router MPU0 %SYS_UPDATE-RESULT-5:pkgInfo : Mpu 0 upgrade
successfully!
 %Sysupdate pkgInfo finished.

      package sysupdate result information list:
--------------------------------------------------------------

rp34-7.7.0.106(R).pck sysupdate result information list:
--------------------------------------------------------------
      Mpu 0  -  upgrade successfully!

rp34-Bootloader-n1-1.0.0.02.pck sysupdate result information list:
--------------------------------------------------------------
      Mpu 0  -  upgrade successfully!

devinfo(v1.14) sysupdate result information list:
--------------------------------------------------------------
      Mpu 0  -  upgrade successfully!

pkg_info.txt sysupdate result information list:
--------------------------------------------------------------
      Mpu 0  -  upgrade successfully!
```

#The above information indicates that the package files of all types of online cards are upgraded successfully.

Note:

- For service board sub card, it will be displayed only when upgrade fails.
- If the command option reload is added, the system prompts whether to save the configuration, and whether to restart the device immediately. However, usually the device is started after all programs are upgraded. Therefore, the reload option is not recommended.
- The router supports IPv6 upgrade; When upgrading with IPv6, ensure that FTP/TFTP supports IPv6 service.

Warning:

- During the upgrade process, you cannot power off the device or swap or restart the main control board. Otherwise, the system may fail to start, or the file may be damaged.

10.3. Typical Configuration Example of Software Upgrade

10.3.1. Upgrade Package File

Network Requirements

- A PC acts as an FTP server, and Device acts as an FTP client. The network between the server and the client is normal.
- On the FTP server, set the user name for a device to log in to the FTP server as admin, and the password as admin. Place the package program to be upgraded in the FTP server directory, and upgrade all software versions of the device that support the package upgrading.

Network Topology

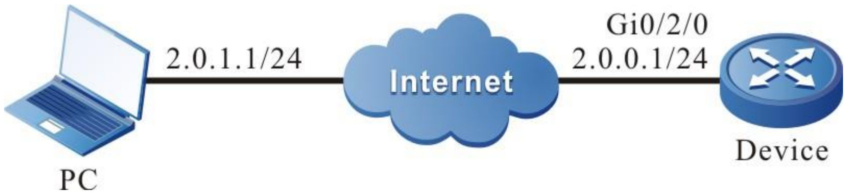


Figure 10-1 Networking for Upgrading all Supported Software Versions in Package

Configuration Steps

Step 1: Configure an FTP server, and place the package upgrade program in the FTP server directory. (Omitted)

Step 2: Back up the device configuration file. (omitted)

Step 3: Configure the IP addresses of the interfaces so that the network between Device and the FTP server is normal. (Omitted)

Step 4: Upgrade the package upgrade program.

#Use sysupdate to upgrade the package upgrade program.

```
Device#sysupdate package 2.0.1.1 rp34-7.7.0.106(R)-001.pkg ftp admin
admin no-comparision
```

After the upgrade is completed, a list of upgrade results will be printed for users to determine the upgrade results of all upgrade programs included in the package upgrade file on the device:

```
          package sysupdate result information list:
--------------------------------------------------------------


rp34-7.7.0.106(R).pck sysupdate result information list:
--------------------------------------------------------------
     Mpu 0   -  upgrade successfully!
```

```
rp34-Bootloader-n1-1.0.0.02.pck sysupdate result information list:
--------------------------------------------------------------
     Mpu 0   -  upgrade successfully!

devinfo(v1.14) sysupdate result information list:
--------------------------------------------------------------
     Mpu 0   -  upgrade successfully!

pkg_info.txt sysupdate result information list:
     Mpu 0   -  upgrade successfully!
```

Warning:

- Before upgrading in package, ensure that all cards are in place and the status is Start OK. During upgrading, do not swap the card, avoiding that the abnormal upgrading of the card affects the subsequent starting of the card.

Note:

- If selecting the "no-comparison" parameter, upgrade the version of the packaged upgrade program directly without image version comparison. If this parameter is not selected, the image version will be compared. If the image version in the packaged upgrade program is lower than the version running on the device or the same as the running version of the device, the device will prompt the user and wait for the user to confirm whether to upgrade the image upgrade program in the package. Whether the user chooses to upgrade the program or not will not affect the upgrade of the other upgrade files in the upgrade package. If there is only the image file in the packaged upgrade package, and the user chooses not to upgrade, the packaged upgrade ends.
- This command can also be added with a "reload" parameter. If the parameter is added, restart the device directly after the upgrade is completed.
- The router supports IPv6 upgrade; When upgrading with IPv6, ensure that FTP/TFTP supports IPv6 service.

Step 5: Use the command to restart the device.

#Use the reload command to restart the device.

```
Device #reload
Save current configuration to startup-config(Yes|No)?y
```

```
Write to startup file ... OK!
Synchronize file /flash/startup succeed.
System will be reloaded!
Please confirm system to reload(Yes|No)?y
```

Warnning:

- Before restarting, whether to save the configuration depends on the actual needs of the user.

Note:

- If the upgrade command contains the “reload” parameter, omit the step.

Step 6: Check the result.

#After completing the upgrade and restarting the device, query the upgraded file version information in the packaged upgrade program via the **show package version** command.

```
Device #show package version


package       :rp34-7.7.0.104(R)-001.pkg
image        :rp34-7.7.0.104(R).pck
Bootloader     :rp34-Bootloader-b2-1.0.0.01.bin
devinfo       :devinfo(v1.14)
```

#Query the version number of the program via the **show system component version** command to check whether it is updated.

```
Device #show system component version


Component version information display:


Component  Name              BootLoader  IOS             CMM          PCB
CPLD     FPGA
-----------------------------------------------------------------------
------------------------------------
Mpu 0     MP2900X-24D(V1)      1.0.0.01    7.7.0.104(integrity)              2
105
Lpu 2     RM2B-4GEF(V1)                                      1
Lpu 3     RM2B-4GET                                         1
Lpu 4      RM2B-1GE                                    1
Power 2
Fan 1
Mpu 0/1    4GE
Mpu 0/3    48GE
```

Warning:

- Query the version of the upgrade file in the packaged upgrade program via the show package version command, and query the final upgrade result via the show system component version command.
- The router supports IPv6 upgrade; When upgrading with IPv6, ensure that FTP/TFTP supports IPv6 service.

10.3.2. Upgrade All Software Versions

Network Requirements

- A PC acts as an FTP server, and Device acts as an FTP client. The network between the server and the device is normal.
- On the FTP server, the user name for a device to log in to the FTP server is admin, and the password is admin. The image program, Bootloader program, CMM program and FPGA program to be upgraded are placed in the FTP server directory. Upgrade all software versions of the device completely.

Network Topology

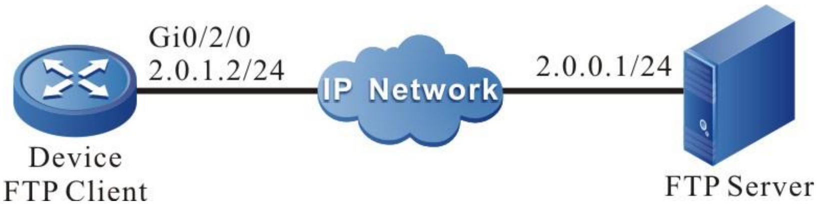


Figure 10-2 Networking for Upgrading All Software Versions

Configuration Steps

Step 1: Configure an FTP server, and place the image program, Bootloader program, and FPGA program in the FTP server directory. (Omitted)

Step 2: Back up device configuration files. (Omitted)

Step 3: Configure the IP addresses of the interfaces so that the network between Device and the FTP server is normal. (Omitted)

Step 4: Upgrade the image program.

#Before upgrading the image program, check whether there is sufficient space in the file system.

```
Device#filesystem
```

```
Device(config-fs)#volume
```

#Use the sysupdate command to upgrade the image program of the active and standby control card.

```
Device#sysupdate image mpu 2.0.0.1 rp34-7.7.0.106(R).pck ftp admin admin
```

For the upgrade procedure of the image program and the print information which indicates whether the upgrade is successful, refer to the "Upgrading the image Program Package" in "Configuring Software Upgrade Functions".

Step 5: Upgrade the Bootloader program.

#Use the sysupdate command to upgrade the Bootloader program of the control card.

```
Device# sysupdate Bootloader mpu 2.0.0.1 rp34-Bootloader-b2-1.0.0.01.pck ftp admin admin
```

For the upgrade procedure of the Bootloader program and the print information which indicates whether the upgrade is successful, refer to the "Upgrading the Bootloader Program" in "Configuring Software Upgrade Functions".

Step 6: Upgrade the FPGA program.

#According to the need, upgrade the FPGA program of POS, E1 and other WAN sub cards. For example: use sysupdate to upgrade the FPGA program of all POS sub cards on the device.

```
Device#sysupdate fpga all 2.0.0.1 ir010pos-oc3_fpv010_110.bin ftp admin admin
```

The upgrade commands of WAN sub cards such as POS and E1 are the same as above, only the file name needs to be modified. For the printing information about the process of upgrading the FPGA program and whether upgrading succeeded, refer to the relevant contents of “Upgrade FPGA” in “Software upgrade function configuration”.

Warning:

- When upgrading FPGA, if the board type is not specified, the corresponding board will be automatically searched according to the FPGA program type for upgrading.
- In general, FPGA program update frequency is relatively low. Please confirm that the upgrade version is newer than the current version of the system before upgrading. Please refer to the following step 10 for viewing the current FPGA version number of the system.

Step 7: Upgrade the CPLD file.

#Use sysupdate to upgrade the CPLD program of the board card.

```
Device# sysupdate cpld mpu 2.0.0.1 pr019_cpld_clv006.pck ftp admin admin
```

For the printing information about the process of upgrading the CPLD program and whether upgrading succeeded, refer to the relevant contents of “Upgrade CPLD” in “Software upgrade function configuration”.

Step 8: Restart the device via the command.

#Use the **reload** command to restart the device.

```
Device #reload
Save current configuration to startup-config(Yes|No)?y
Write to startup file ... OK!
Synchronize file /flash/startup succeed.
Warnning:
System will be reloaded!
Please confirm system to reload(Yes|No)?y
```

Before the restart, determine whether to save the configuration according to the actual requirement.

Step 9: Check the result.

#After the upgrade is completed and the device is restarted, view the version numbers of the programs to check whether the versions have been upgraded.

#Check whether the image and Bootloader programs of the control cards have been upgraded successfully.

```
Device#show  system  mpu
System MPU Information (Mpu 0 - ONLINE)
---------------------------------------------------------
             Type: MP2900X-24D(V1)[0x10431386]
             Role: Master
         Auth Status: Auth Ok
         Local Status: Start Ok
        Global Status: Start Ok
       Card-SubSlot-Num: 3
      Power-Card-Status: On
          Serial No:
          Card-Name: MP2900X-24D(V1)
         Description:
Hardware-Information:
         PCB Version: 2
Temperature-RT-Information:
       CPU Temperature: 51 C
      Switch Temperature: 75 C
CPU-On-Card-Information:   < 1 CPUs>
           Core Num: 2
       coreUtilization: 17.00%
MEM-On-Card-Information:   < 1 MEMs>
```

```
            Free(KB): 376128
           Total(KB): 1002944
       Utilization Ratio: 62.49%
 DISK-On-Card-Information:  < 1 DISKs>
            Disk-Idx: 0
              Type: 1
             Status: 1
            SizeTotal: 4621615104
            SizeFree: 3693203456
 IOS-On-Card-Information:  < 1 IOSs>
          Ios Version: 7.7.0.104(integrity)
 BOOT-On-Card-Information:  < 1 BOOTs>
          Boot Version: 1.0.0.01
 CPLD-On-Card-Information:  < 1 CPLDs>
          Cpld Version: 105
---------------------------------------------------------------

System MPU Information (Mpu 0/1 - ONLINE)
---------------------------------------------------------------
              Type: 4GE[0x10131304]
          Auth Status: Auth Ok
          Local Status: Start Ok
         Global Status: Start Ok
---------------------------------------------------------------

System MPU Information (Mpu 0/3 - ONLINE)
---------------------------------------------------------------
              Type: 48GE[0x10131330]
          Auth Status: Auth Ok
          Local Status: Start Ok
         Global Status: Start Ok
---------------------------------------------------------------
```

#Verify whether the FPGA program upgrade of the service board is successful.

```
Device#show  system  lpu 1
System LPU Information (Lpu 1 - ONLINE)
---------------------------------------------------------------
```

```
                  Type: RM2B-4CE1(V2)[0x1320a004]
           Auth Status: Auth Ok
          Local Status: Start Ok
         Global Status: Start Ok
      Card-SubSlot-Num: 0
     Power-Card-Status: On
             Serial No: 7878787878787878
             Card-Name: RM2B-4CE1(V2)
           Description:
                Uptime: 5 days 3 hours
Hardware-Information:
           PCB Version: 1
FPGA-On-Card-Information:  < 1 FPGAs>
          Fpga Version: 103
-------------------------------------------------------------
```

The **show system lpu** command will display the relevant information of all the service cards in place. Here, only the relevant information of the service card (Lpu 1) in slot 1 is listed. The relevant information of the service cards in other slots is omitted here.

<u>Note:</u>

- The reachable interface between the device and the FTP server can be the ge0, ge1, ge2, ge3 out-of-band management interface or the service interface.
- It does not matter whether the Bootloader program, the Bootloader or FPGA program is upgraded first, but the device can be restarted only after all programs have been upgraded.
- Before the upgrade, ensure that there is sufficient space in the flash file system of the main control card for saving the image file that is used for upgrade. If there is not sufficient space on the device, delete the files that are not in need from the file system of the device. The remaining flash space of the main control card is recommended to be larger than 170M before the upgrade. Otherwise, the upgrade time may become longer.
- If some programs in the newly released version have not changed, the unchanged programs cannot be upgraded.
- In the process of upgrading, if some boards fail to upgrade due to abnormal conditions, they can be upgraded separately.
- The router supports IPv6 upgrade; When upgrading with IPv6, ensure that FTP/TFTP supports IPv6 service.

10.3.3. Upgrade the Bootloader Program via the Console Port

Network Requirements

- PC and the Console port of the device are directly connected.
- The Bootloader program of the control cards is to be upgraded through the Console port.

Network Topology

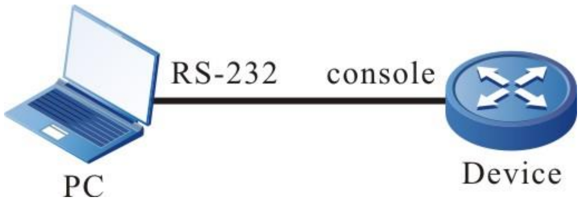


Figure 10-3 Upgrading the Bootloader Program via the Console Port

Configuration Steps

Step 1: Connect PC and the Console port of the device properly.(Omitted)

Step 2: Open the Bootloader screen.

When the device is just started and the " Press ctrl+c to enter Bootloader mode: 0 " message is printed, press and hold **Ctrl + C** to open the Bootloader screen.

Step 3: Set the transmission rate to 115200 bps to improve the upgrade speed.

```
Bootloader#srate 115200
```

#After setting the transmission speed of the Console port of Bootloader, you should set the transmission speed of the HyperTerminal also to 115200 bps.

Step 4: On the Bootloader screen, upgrade the Bootloader version.

```
Bootloader#mupdate Bootloader
```

#Input the **mupdate Bootloader** command, and use ymodem to transmit the Bootloader file that has been saved on the PC.

#Check the result.

#After upgrading, print the following information on the Bootloader interface.

```
Protected 39 sectors
Update Bootloader OK.
Bootloader#
```

Step 5: Check the result.

#After the upgrade is completed and the device is restarted, the system is booted by the new Bootloader, and the following message is printed:

```
Bootloader 1.0.2.03 compiled at Aug 30 2019,10:55:39
Warm boot from master sector
cpu reboot lbootext:0x0 lboot:0x1 cpld reboot:0x00000040
```

Note:

- Upgrade through the Console port is complex and slow, so the TFTP/FTP upgrade mode is recommended. The Console port upgrade mode is used only when the upgrade conditions of the TFTP/FTP upgrade mode fail to be satisfied.
- After the upgrade is completed, use the **reset** command to exit Bootloader program. Then, the new Bootloader program boots the loading of the image program.

- If the default rate of the Console port has been modified in upgrading the Bootloader program, in loading the image program package, the rate of the device Console port automatically resumes to 9600 bps. At this time, the rate of the HyperTerminal needs to be modified synchronously.

11. BOOTLOADER

11.1. Overview

In an embedded system, Bootloader runs before the Operating System (OS) kernel runs. Bootloader is used to initialize hardware devices (including the Console port, Ethernet port, and flash), and set up memory space mapping to bring the hardware and software of the system to a proper state. Finally, it prepares a proper environment for booting the OS kernel. In the embedded system, there is no such firmware program as BIOS, so the booting of the entire system is implemented by the Bootloader.

The Bootloader system mainly provides the following functions:

- Sets startup parameter, load and run the specified image program, and select the loading mode of the Image program.
- Upgrades the Bootloader program.

11.2. Bootloader Function Configuration

Table 11-1 Bootloader function configuration list

Configuration Tasks	
Set the Bootloader boot parameters	Set the Bootloader boot parameters
Clear up the configuration file of the device system	Clear up the configuration file of the device system
Upgrade the Bootloader program	Upgrade the Bootloader program

11.2.1. Preparation before Configuring the Bootloader Functions

Before configuring the Bootloader functions, you need to set up a local configuration environment. Connect the Console port of the host (or terminal) to the Console port of the device through a configuration cable. The configuration of the communication parameters of the host (or terminal) must be the same as the default configuration of the Console port of the device. The default configuration of the Console port of the device is as follows:

- Transmission speed: 9600 bps
- Flow control mode: None
- Check mode: None
- Stop bit: 1 bit
- Data bit: 8 bits

11.2.2. Set the Bootloader Boot Parameters

Configuration Condition

None

Set Bootloader Boot Parameters

Table 11-2 Set the Bootloader boot parameters

Step	Command	Description
Enter the Bootloader configuration mode	None	Mandatory. After the device is powered on, press the Ctrl + C keys to enter the Bootloader configuration mode. After you enter the mode, the "bootloader#" is prompted.
Set the boot parameters of Bootloader	**change** { *index* } { *boot-dev* } { *filename* } [*local-ip-addr*] [*host-ip-addr*] [*gatewayip*] [*netmask*]	Mandatory

Note:

- If you set the boot device type as file system boot, you can select the name of the image program that currently exists in the flash file system to load and run according to the prompt information.
- If the boot device type is set to network boot, after configuring the boot parameter information, first of all, you need to ensure that route between the Ethernet interface of the host or terminal and the network management interface of the device (such as ge0, ge1, ge2, ge3) is reachable. You can use the ping tool to ping the IP address of the device end at the host end to detect whether the network channel is connected normally.

11.2.3. Clear Configuration File of Device System

Configuration Condition

None

Clear Configuration File of Device System

Table 11-3 Clear the configuration file of the device system

Step	Command	Description
Enter the Bootloader configuration mode	None	Mandatory. After the device is powered on, press the Ctrl + C keys to enter the Bootloader configuration mode. After you enter the mode, the "bootloader#" is prompted.

Step	Command	Description
Clear the configuration file of the device system	**delete** [*startup*]	Mandatory

Note:

- If the configuration file is /flash/startup, delete startup will delete the configuration file and back up the startup file.
- Back up startup as a system file for device configuration recovery, which is invisible to users and can only be deleted by the delete command.
- If the device startup file and backup startup file are deleted, when the device loads and runs the image program, no configuration file will be executed, that is, the system has no configuration.

11.2.4. Upgrade the Bootloader Program

Configuration Condition

None

Upgrade the Bootloader Program

Table 11-4 Upgrade the Bootloader program

Step	Command	Description
Enter the Bootloader configuration mode	None	Mandatory. After the device is powered on, press the Ctrl + C keys to enter the Bootloader configuration mode. After you enter the mode, the "PMON>" is prompted.
Start the tftp service on the PC		Mandatory Copy the new Bootloader version used for upgrading to the root directory of tftp, used by the device to download the version file via tftp.
Upgrade the Bootloader program	**update Bootloader***filename* **dc0** *local-ip-addr host-ip-addr [gatewayip] [netmask]*	Mandatory
Back up the Bootloader program	**Bootloaderbak**	Optional

Note:

- Bootloader system program adopts dual-Bootloader backup mode, which is divided into the master Bootloader program and standby Bootloader program. With the upgrade command, you can only upgrade the version of the master Bootloader, while the standby Bootloader program will remain unchanged.
- After upgrading the Bootloader system program, use the command reset or power off to restart the device, and then, you can use the latest Bootloader system program.
- After the system is loaded successfully, you can use the **sysupdate** command to upgrade.

11.3. Typical Configuration Example of Bootloader

11.3.1. Configure Bootloader to Guide Image Program from File System

Network Requirements

None

Network Topology

None

Configuration Steps

#Enter the command **change** to set bootloader parameter 0, select to load and run image program rp34-7.3.0.7.34(R).pck from the file system of the device flash 0.

```
bootloader# change 0 flash0 rp34-7.3.0.7.34(R).pck
 1 bytes read in 0 ms
 print index:0 boot param info:
        boot dev: flash0
        boot file: rp34-7.3.0.7.34(R).pck
```

#Input the command **boot** to start guiding the Image program.

```
bootloader#boot
```

11.3.2. Configure Bootloader to Guide Image Program from Network

Network Requirements

- PC acts as the TFTP server, and the device acts as the TFTP client; the server is connected to the device network.
- Put the bootloader program to be upgraded in the TFTP server directory to upgrade the bootloader version of the device.

Network Topology

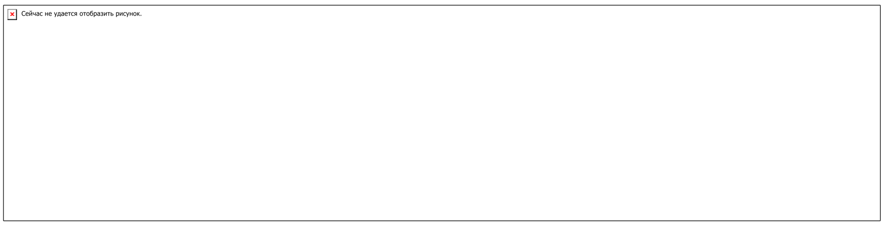


Figure 11-1 Networking of upgrading the bootloader version

Configuration Steps

#Input the command **change** to set boot parameter 0 of bootloader, set boot parameter o of bootloader, select to load and run the image program rp34-7.3.0.7.34 (R). pck from the network management interface ge0 of the device; Set the IP address of ge0 as 2.0.1.2; Set the host IP address of TFTP server to 2.0.0.1 and the device gateway address to 2.0.1.1.

```
bootloader# change 0 ge0 rp34-7.3.0.7.34(R).pck 2.0.1.2 2.0.0.1 2.0.1.1 255.255.255.0
print index:0 boot param info:
    boot dev: ge0
    boot file:  rp34-7.3.0.7.34(R).pck
    boot local ip: 2.0.1.2
    boot host ip: 2.0.0.1
    boot gatewayip: 2.0.1.1
    boot netmask: 255.255.255.0
```

#Input the command **boot** to guide the image program loading.

```
bootloader#boot
```

12. POE MANAGEMENT

12.1. Overview

The existing Ethernet, with its basic structure of Cat.5 cabling unchanged, not only transmits data signals for IP-based terminals (such as IP phones, WLAN access points, and network cameras), but also provides the DC power supply for the devices. This technology is called Power over Ethernet (PoE). The PoE technology ensures not only the security of existing structured cabling but also normal operation of the existing network, greatly reducing the cost.

PoE is also called Power over LAN (PoL) or Active Ethernet. It is the latest standard specification for making use of existing standard Ethernet transmission cable to transmit data and provide power. It is compatible with the existing Ethernet systems and users. IEEE 802.3af and IEEE802.3at are the technical standards that PoE must comply with. IEEE802.3af is the basic standard of the PoE technology. It is based on the IEEE 802.3, and the standards related to direct power supply through network cables are added. It is an extension of the existing Ethernet standards. IEEE802.3at is an extension based on the IEEE802.3af.

According to the definition of the IEEE802.3af standard, a complete PoE power supply system consists of two types of devices: Power Sourcing Equipment (PSE) and Power Device (PD).

- PSE: It provides power to other devices.
- PD: Devices that receive power. The power of the devices is usually not large.

12.1.1. PSE/PD Interface Specifications

For the 10BASE-T and 100BASE-TX IEEE802.3af networks, IEEE802.3af defines Power Interfaces (PIs), which are interfaces between PSE/PD and network cables. Currently, it has defined two power supply modes, Alternative A (1, 2, 3, 6 signal wire pairs) and Alternative B (idle wire pairs 4, 5, 7, and 8). The following is a description of the two power supply modes:

1. Power supply through signal wire pairs (Alternative A)

As shown in the following figure, a PSE can supply power to a PD through signal wire pairs. Because DC and data frequency does not interfere with each other, electric current and data can be transmitted through the same wire pair. For electric cables, this is a kind of "multiplexing". Wires 1 and 2 are connected to form a positive (or negative) polarity, and wires 3 and 6 are connected to form a negative (or positive) polarity.

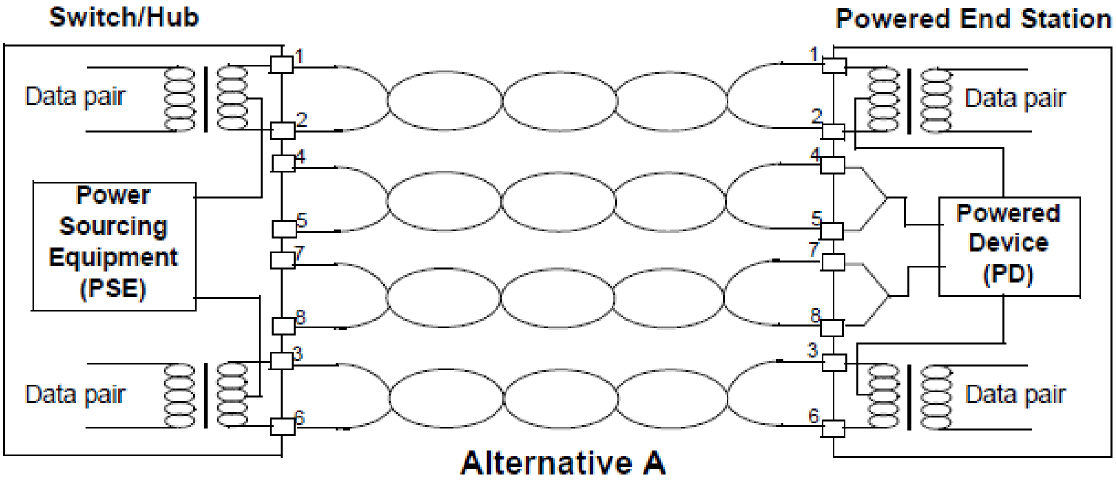


Figure 12-1 Alternative A Power Supply Mode with 10BASE-T and 100BASE-TX

2. Power supply through idle wire pairs (Alternative B)

As shown in the following figure, a PSE can supply power to a PD through idle wire pairs. Wires 4 and 5 are connected to form a positive polarity, and wires 7 and 8 are connected to form a negative polarity.

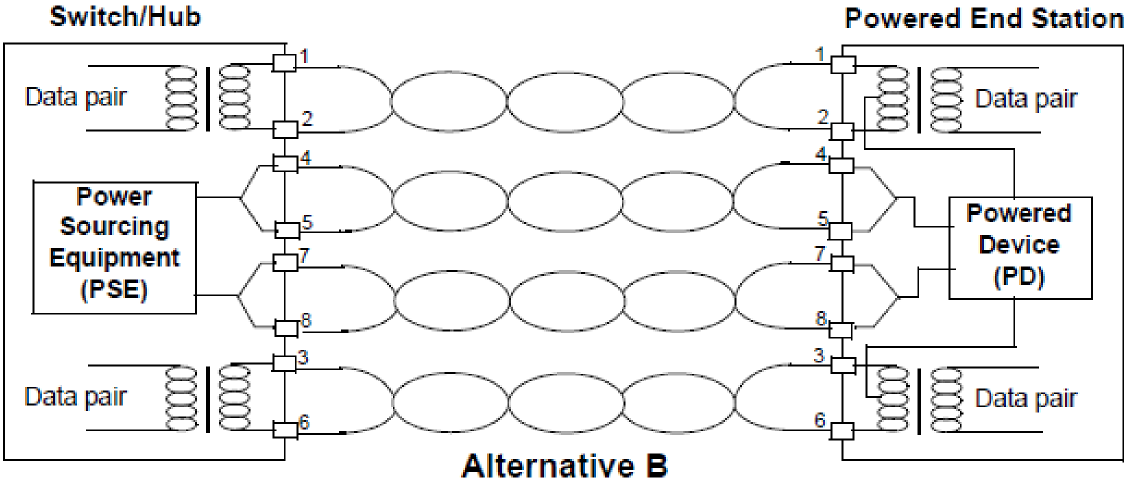


Figure 12-2 Alternative B Power Supply Mode with 10BASE-T and 100BASE-TX

According to IEEE802.3af, standard PDs must support both power supply through signal wire pairs and power supply through idle wire pairs, while PSEs need only support either of the two modes.

12.1.2. PoE Power Supply Process

If a PSE is installed in a network, the PoE Ethernet power supply process is as follows:

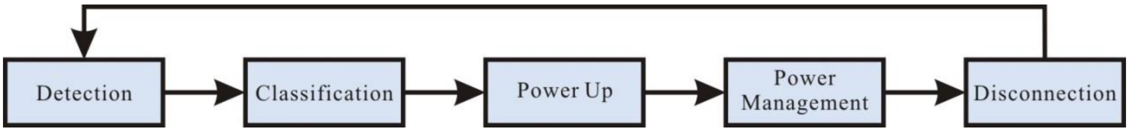


Figure 12-3 PSE Power Supply Process

- Detection: After a network device is connected to a PSE, the PSE first detects whether the device is a PD to ensure that the current is not supplied to non-PDs because supplying power to a device that is not a PD may damage the device. The PSE detects the resistance capacitance between the power output wire pairs to determine whether PDs exist. The PSE proceeds to the next step only after it detects PDs.
- Classification: After detecting PDs, the PSE classifies the PDs. It determines power grade of PDs by detecting power output current. During the power supply process, classification is optional.
- Power Up: Within a startup period which is configurable (usually less than 15 us), the PSE starts to provides low power voltage to PDs and gradually increases the power voltage to 48 V DC.
- Power Management: The PSE provides stable and reliable 48 V DC power for PDs. Once the PSE starts to supply power, it continuously detects PD current inputs. If the current consumption of a PD drops under the minimum value owing to various causes, such as the PD is disconnected, the PD encounters power consumption overload or short circuit, and the power load exceeds the PSE power supply load, the PSE regards the PD as not in position or abnormal. In this case, the PSE stops providing power to the PD.

- Disconnection: The PSE detects the current of PDs to determine whether PDs are disconnected. If a PD is disconnected, the PSE stop supplying power to the PD quickly (usually within 300 to 400 ms), and then the PSE returns to the Detection status.

12.2. PoE Function Configuration

Table 12-1 PoE Function List

Configuration Tasks	
Configure PoE basic functions.	Enable the global PoE function.
	Enable the interface PoE function.
	Enable the forced power supply function of an interface.
Configure the PoE power.	Configure the total power of PoE.
	Configure the protection power of PoE.
	Configure the maximum output power limit mode of an interface.
	Configure the maximum output power of an interface.
Configure power supply priorities.	Configure a PoE power management mode.
	Configure the power supply priority of an interface.
Configure PD power-on parameters.	Configure the PD detection mode of an interface.
	Configure the interface classification mode.
	Configure the power-on impulse current mode of an interface.
Configure the abnormality recovery function.	Configure the time for recovery from a power supply abnormality of an interface.
	Restart the PoE power supply.
Configure the POE power alarm function	Configure the PoE power alarm threshold

12.2.1. PoE Basic Function Configuration

The PoE function is controlled by configuring global PoE and interface PoE, that is, the PoE function can be used only when the global PoE and interface PoE are both enabled. If you run the command for disabling the global PoE, the PoE functions of all interfaces are disabled. If you run the command for disabling the interface PoE function, you can choose to disable the PoE function of some interface. The interface PoE function is a standard power supply mode, while the interface forced power supply function is a special power supply mode. You can select only one mode at a time. However, both of the two modes are valid only after the global PoE function is enabled.

Configuration Condition

None

Enable the Global PoE Function

Table 12-2 Enabling the Global PoE Function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the global PoE function.	**power enable**	Optional. By default, the global PoE function is enabled.

Enable the Interface PoE Function

Table 12-3 Enabling the Interface PoE Function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the global PoE function.	**power enable**	Optional. By default, the global PoE function is enabled.
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	-
Enable the interface PoE function.	**power enable**	Optional. By default, the interface PoE function is enabled.

Enable the Forced Power Supply Function of an Interface

Table 12-4 Enabling the Forced Power Supply Function of an Interface

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the global PoE function.	**power enable**	Optional. By default, the global PoE function is enabled.
Enter the L2 Ethernet interface configuration mode.	**interface** *interface-name*	-
Enable the forced power supply function of an interface.	**power force** { **always** | **once** }	Mandatory. By default, the forced power supply function of an interface is disabled.

Note:

- Forced power supply is a special power supply mode, which does not require enabling the interface PoE function.

12.2.2. Configure PoE Power

Configuration Condition

Before configuring the PoE power, ensure that:

- The global PoE function is enabled.
- The interface PoE function is enabled.

Configure Total Power of PoE

By configuring the total power of PoE, you can limit maximum output power of the device. If the total power required by all PDs exceeds the configured total power, power supply to some PDs is stopped according to the current power supply priority mode.

Table 12-5 Configuring the Total Power of PoE

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-

Step	Command	Description
Configure the total power of PoE.	**power total-power** *power-value*	Optional. By default, the total power is the maximum total power that the device power supply can provide.

Configure the Protection Power of PoE

When a PD is normally powered, the consumed power fluctuates within a certain range. To prevent PD power-off owing to power fluctuation, part of power is reserved from the total power of the device to act as the protection power. When the consumed power of the PD increases, the increased part is allocated from the protection power.

Protection power may also be allocated as normal power supply. When the available power is insufficient for providing power to newly connected PDs, if the available power of the device and the protection power is equal to or larger than the maximum output power of the interface of the new PD, sufficient power is allocated from the protection power to the new PD.

Table 12-6 Configuring the Protection Power of PoE

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the protection power of PoE.	**power guard-band** *guard-band-value*	Optional. By default, the protection power of the power supply is 40.0 watt.

Configure the Maximum Output Power Limit Mode of an Interface

The maximum output power of an interface is determined by the PD classification type. You can also customize the maximum output power of an interface.

Table 12-7 Configuring the Maximum Output Power Limit Mode of an Interface

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	-

Step	Command	Description
Configure the maximum output power limit mode of an interface.	**power threshold-mode** { **classification** | **user** }	Optional. By default, the maximum output power limit mode is the user customization mode.

Configure the Maximum Output Power of an Interface

You can limit the maximum power that a PSE can supply to a PD through an interface. If the power required by a PD exceeds the maximum output power of the interface, the PSE stops power supply to it.

Table 12-8 Configuring the Maximum Output Power of an Interface

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	-
Configure the maximum output power limit mode to the user customization mode.	**power threshold-mode user**	Mandatory. By default, the maximum output power limit mode is the user customization mode.
Configure the maximum output power of an interface.	**power port-max-power** *max-power-value*	Optional. By default, the maximum output power is 30.0 watt.

12.2.3. Configure Power Supply Priorities

With the power supply priority function, if the total power of a PSE is insufficient for powering all PDs, key PDs have the priority to obtain power. Through this function, you can configure the mode in which key PDs are powered.

Configuration Condition

Before configuring power supply priorities, ensure that:

- The global PoE function is enabled.
- The interface PoE function is enabled.

Configure a PoE Power Management Mode

Table 12-9 Configuring a PoE Power Management Mode

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure PoE power management mode.	**power manage** { **dynamic-fifs** | **dynamic-priority** }	Optional. The default power management mode is the dynamic First In First Served (FIFS).

Configure Power Supply Priority of an Interface

If the PoE power management mode is the dynamic priority mode, when the power supply of the PSE is insufficient, the PD that is connected to the interface with a higher power supply priority is first powered. If the power supply priorities of the interfaces are the same, the PD that is connected to the interface with smaller number is powered first.

Table 12-10 Configuring the Power Supply Priority of an Interface

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the PoE power management to dynamic priority.	**power manage** **dynamic-priority**	Optional. The default power management mode is the dynamic priority.
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	-
Configure the power supply priority of an interface.	**power priority** { **critical** | **high** | **medium** | **low** }	Optional. The default power supply priority is low.

12.2.4. Configure PD Power-On Parameters

PoE power-on process falls into the following stages:

1. Detection: The PSE detects whether PDs exist.
2. Classification: The PSE grades PDs and determines power consumption of PDs. This stage is optional.
3. Power-Up: The PSE supplies power to PDs.

You can adjust the parameters set for the previous stages and supply power to PDs of different types.

Configuration Condition

Before configuring PD power-on parameters, ensure that:

- The global PoE function is enabled.
- The interface PoE function is enabled.

Configure PD Detection Mode of an Interface

After the PoE function of an interface is enabled, the PSE detects the resistance capacitance between the power output wire pairs to determine whether PDs exist. The standard detection mode detects only PDs that comply with IEEE802.3af and IEEE802.3at. The standards define PDs and non-PDs, but there is a type of devices with resistance capacitance between those of PDs and non-PDs. The compatible mode can detect this type of devices.

Table 12-11 Configuring the PD Detection Mode of an Interface

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	-
Configure the PD detection mode of an interface.	**power detect-mode** { **compatible** | **standard** }	Optional. The default PD detection mode is the standard mode.

Configure the Interface Classification Mode

After the interface PoE function is enabled, the PSE detects the output current of the power supply to determine the power grades of PDs. Power is allocated to PDs according to the power grades of the PDs. PD classification is an optional step. You can skip the step by setting the non-classification mode.

Table 12-12 Configuring the Interface Classification Mode

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	-
Configure the interface classification mode.	**power class-mode** { **standard** | **never** }	Optional. By default, no classification is support.

Note:

- Some non-standard PDs may not support classification. This type of PDs are classified to class0 by default, and the maximum output power of the interface is 15.4 watt.

Configure Power-On Impulse Current Mode of an Interface

The PoE standard defines the PD power-on impulse current. The parameter is related to PSE, (parasitic) capacitance of the PD, and power of the PD. For the PDs that comply or not comply with the standard, the required power-on impulse current may be different. For different PDs, the related power-on impulse current mode must be configured.

Table 12-13 Configuring the Power-On Impulse Current Mode of an Interface

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	-
Configure the power-on impulse current mode of an interface.	**power power-up-mode** { **802.3af** | **high** | **Pre-802.3at** | **802.3at** }	Optional. The default power-on current mode is high.

12.2.5. Configure Abnormality Recovery Function

When there is a PoE power supply abnormality, the abnormality recovery function is supported, including automatic recovery and manual recovery.

Configuration Condition

Before configuring the abnormality recovery function, ensure that:

- The global PoE function is enabled.
- The interface PoE function is enabled.

Configure the Time for Recovery from a Power Supply Abnormality of an Interface

If a PSE detects abnormal power supply status of an interface while powering PDs, it automatically disables the PoE function of the interface. After the time for recovery from a power supply abnormality elapsed, it enables the PoE function again, and tries to supply power to the PD of the interface.

Table 12-14 Configuring the Time for Recovery from a Power Supply Abnormality of an Interface

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	-
Configure the time for recovery from a power supply abnormality of an interface.	**power recover-time** *time-value*	Optional. By default, the time for recovery from a power supply abnormality is 0 minute, indicating recovery immediately.

Restart PoE Power Supply

When a PoE power supply abnormality occurs or the PoE power supply is abnormal, you can manually hot restart the PoE power supply to try to recover from the abnormal status.

Table 12-15 Configuring the Time for Recovery from a Power Supply Abnormality of an Interface

Step	Command	Description
Restart the PoE power supply.	**power reload**	Mandatory.

Note:

- In the process of power restarting, execute the **power reload** command again and prompt the execution failure.

12.2.6. Configure PoE Power Alarm Threshold

Configuration Condition

Before configuring the PoE power, first complete the following task:

- Enable global PoE function
- Enable interface PoE function

Configure PoE Power Alarm Threshold

When the PoE power utilization reaches or is lower than the set power threshold, send the Trap alarm prompt.

Table 12-16 Configure the PoE power alarm threshold

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the PoE power alarm threshold	**power alarm-threshold** *threshold-value*	Optional By default, the power alarm threshold is 99%.

12.2.7. PoE Monitoring and Maintaining

Table 12-17 PoE Monitoring and Maintaining

Command	Description
show power { **manage** | **summary** | **configure interface** *interface-name* | **detect interface** *interface-name* | **pd-status interface** *interface-name* | **version** }	Display the PoE configuration, the power supply status information, and the power corresponding relation information.

13. LUM

13.1. Overview

LUM (Local User Manager): The local user database used to provide the AAA local authentication.

RBAC (Role Based Access Control): By establishing the association of "Authority <-> Role", assign the authority to the role, and by establishing the association of "Role <-> User", specify the role for the user, so that the user can get the authority of the corresponding role. The basic idea of RBAC is to specify roles for users. These roles define which system functions and resource objects the users are allowed to operate.

Because of the separation of the authority and the user, RBAC has the following advantages:

- The administrator does not need to specify authorities one by one for users, they just need to define the roles with corresponding authorities in advance, and then assign the roles to users. Therefore, RBAC can better adapt to the changes of users and improve the flexibility of user authority allocation.
- Because the relationship between roles and users often changes, but the relationship between roles and authorities is relatively stable, so using this stable association can reduce the complexity of user authorization management and management cost.

Role: The set of rules

Rule: The permit/deny authority of the commands of the specified features or all features

Feature: Module

13.2. LUM Function Configuration

Table 13-1 LUM function configuration list

Configuration Task	
Configure the user role	Configure the user role
Configure the administrator scheme	Configure the administrator
	Configure the administrator user group
Configure the access user scheme	Configure the access user
	Configure the user group

13.2.1. Configure the Role

By default, there are four roles: Security-admin, Network-admin, Audit-admin and Network-operator. The authorities of these four roles cannot be changed.

Customize role authorities as a subset of network administrator role authorities. It is not allowed to configure module authorities that have been granted security-admin and auditor-admin roles. For detailed authorities, refer to the following table:

Table 13-2 The corresponding authorities of the user roles

	Log	**History**	**User management, user authentication**	**Other Modules**
Public	NO	NO	Modify own password	Show running, exit and so on
Security-admin	Operation log query and related configuration commands	History configuration and operation	OK	Lai module, line , service, AAA
Audit-admin	Data log query and configuration commands	NO	NO	NO
Network-admin	All other commands except for the operation log and data log	History configuration and operation	NO	OK
Network-operator	All show commands in the network administrator authority	Show command	NO	All show commands in the network administrator authority

By default, the user does not configure the role attribute. When the role attribute takes effect, the user level does not take effect any more, and the role replaces the user level as the basic criterion of instruction authorization: users have the execution authorities of different instructions according to their roles.

Configuration Conditions

None

Configure User Roles

Table 13-3 Configure the user role

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Create one user role and enter the user role mode	**role** *role-name*	Mandatory By default, there are four roles: Security-admin, Network-admin, Audit-admin and Network-operator. The authorities of these four roles cannot be changed.
Create a rule for the user role	**rule** *number* **{ deny | permit } feature {all** | *feature-name* }	By default, do not define a rule for the new user role, that is, the current user role has no authorities. The rule modification does not take effect for the current online user, but takes effect for the future user that logs in and uses the rule of the role. The smaller the rule ID, the higher the rule priority.

13.2.2. Configure the Local User

Local users are the users stored in devices: including local administrators and local access users. Only when the authentication method is local will it take effect. When you create a local user, you specify whether it is an administrator or an access user.

Configuration Conditions

None

Configure Local Administrator User

Table 13-4 Configure the administrator

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Create an administrator user and enter the administrator user mode	**local-user** *user-name* **class manager**	Mandatory By default, do not configure the administrator user.

Configure Local Access User

Table 13-5 Configure the access user

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Create an access user and enter the access user mode	**local-user** *user-name* **class network**	Mandatory By default, do not configure the access user.

13.2.3. Configure Administrator User Attribute

The administrator indicates the user logging into the device.

When configuring the attribute of the local administrator user, there are the following configuration restrictions and instructions:

- If the user authorizes the role through AAA at the time of login, whether the user can execute the command after logging to the device depends on the role. If not authorizing the role through AAA at the time of login, whether the user can execute the command after logging into the device depends on the user level.
- For SSH users, when using public key authentication, when the authentication mode of logging into the device is not configured in the user line view, the commands they can use are based on the user role or user level set in the local administrator user view with the same name as the SSH user (the priority of the user role is higher than the user level). For the detailed introduction to user roles, refer to “Configuration Roles” in “LUM Configuration Guide”.
- The maximum try times of the user password can be configured in the local administrator user view and administrator user group view. The priority order of the configuration in each view is: local administrator user view - > administrator user group view.

- The password lifecycle of the user can be configured in the local administrator user view, the administrator user group view and the global view. The priority order of the configuration in each view is: local administrator user view - > administrator user group view - > global view.

Configuration Conditions

None

Configure the Attribute of Administrator User

Table 13-6 Configure the attribute of the administrator user

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Create an administrator user and enter the administrator user mode	**local-user** *user-name* **class manager**	Mandatory By default, do not create the administrator user.
Configure the administrator user password	**password 0** *password*	Mandatory By default, the user does not have password.
Set the server type that the user can adopt	**service-type { ssh | telnet | console |ftp | web | netconf }**	Mandatory By default, the user does not support any service-type.
Set the user role of the local user	**user-role** *role-name*	Optional By default, do not configure the administrator role. The priority of the administrator role is higher than the administrator level, that is, when the administrator user is configured with the role, the administrator authority is based on the administrator role.

Step	Command	Description
Set the user group of the administrator user	**group** *group-name*	Optional By default, do not configure the user group.
Configure the level of the login user authorization	**privilege** *privilege-level-number*	Optional By default, the default level is 1.
Configure the command that the user automatically executes	**autocommand** *command-line*	Optional By default, do not configure the command that the user automatically executes.
Configure the option that the user automatically executes the command	**autocommand-option** { **nohangup** [**delay** *delay-time-number*] |**delay** *delay-time-number* [**nohangup**] }	Optional By default, disconnect after executing the command automatically and the delay time of automatically executing the command is 0.
Configure the life period of the user	**password-control livetime** *user-live-time*	Optional By default, do not limit the life period of the user.
Configure the maximum times of the successive login authentication failure of the administrator user	**password-control max-try-time** *max-try-time-number*	Optional By default, the user management does not limit the maximum try times.
Configure the maximum online quantity of one user	**max-online-num** *user-number*	Optional By default, do not limit the maximum online quantity of one user.

Step	Command	Description
Configure the file authority that the user can use	**filesys-control{read | write | execute | none}**	Optional By default, the user owns the read, write, and execute file authorities.
Configure the directory provided by the device for the administrator to access or manage	**work-directory** *directory*	Optional By default, it is /flash directory. Currently, the attribute only functions on the file directory of configuring ftp user login device.

13.2.4. Configure Access User Attribute

The access user is the user that is connected to the network via the device.

Configuration Conditions

None

Configure the Access User

Table 13-7 Configure the access user

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Create one access user and enter the access user mode	**local-user** *user-name* **class network**	Mandatory By default, do not configure the access user.
Configure the access user password	**password 0** *password*	Mandatory By default, the user does not have password, and as a result, maybe the user cannot log into the device.

Step	Command	Description
Set the server type that the access user can use	**service-type** { **ppp** / **xauth**}	Mandatory By default, the user does not support any service-type.
Set the user group of the access user	**group** *group-name*	Optional By default, do not configure the user group of the access user.
Specify the DNS address for the remote device	**remote-settings dns** *dns-address1* [*dns-address2*]	Optional By default, do not specify the DNS address for the remote device.
Specify the assignable IP address for the remote device	**remote-settings ip address** *ip-address ip-mask*	Optional By default, do not assign the IP address for the remote device.
Specify the WINS address for the remote device	**remote-settings wins** *wins-address1* [*wins-address2*]	Optional By default, do not specify the WINS address for the remote device.
Configure the user status	**stat** { **active** / **block** }	Optional By default, the status of the user is active.

13.2.5. Configure the Local User Group

Local users are divided to administrator user group and access user group.

Administrator user group is a set of administrator user attributes, which supports configuring password lifetime and the maximum number of successive login authentication failures.

Access user group is the management of access users, with hierarchical nesting, which more vividly reflects the organizational structure of the company or department. The access user group does not support any access user attributes.

Configuration Conditions

None

Configure Administrator User Group

Table 13-8 Configure the administrator user group

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Create an administrator user group and enter its mode	**manager-group** *group-name*	Mandatory By default, do not configure the administrator user group.
Configure the lifetime of the user password in the administrator user group	**password-control livetime** *user-live-time*	Optional By default, do not limit the lifetime of the administrator user in the user group, that is, give priority to the password lifetime configured in the administrator user view.
Configure the maximum times of the user successive login authentication failure in the administrator user group	**password-control max-try-time** *max-try-time-number*	Optional By default, do not limit the times of the user successive login authentication failure in the administrator user group, that is, give priority to the maximum times of the successive login authentication failure configured in the administrator user view.

Configure Access User Group

Table 13-9 Configure the access user group

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Create an access user group and enter its mode	**user-group** *group-name*	Mandatory By default, do not configure the access user group.
Configure the parent group of the access user group	**parent** *group-name*	Optional By default, the default parent group is the parent path in the group name path.
Configure the address pool of the access user group	**pool** *pool-name*	Optional By default, there is no address pool in the access user.

13.2.6. Configure the Password Policy

For our system, there is a strong password security policy. Ensure the password security from the complexity of the password, force to modify the password for the initial login, and maximum try times of the password. Password security policy is only valid for local administrator users.

Password complexity:

1. The minimum password length limit allows administrators to limit the minimum password length for administrators. When setting a user password, the system will not allow the password to be set if the length of the password entered is smaller than the set minimum length. And prompt: " Bad password:it is too short."
2. Password combination detection function: The administrator can set the combination type of user password components. The elements of a password include the following four types:

- Capital letters: A-Z
- Lowercase letters: a-z
- Decimal digits: 0-9
- 31 Special Characters: (`~!@$%^&*()_+-={}[]|\:;”’<>,./’)

There are four combination types of password elements, which have the following specific meanings:

- Combination type 1 indicates that there is at least one element in the password.
- Combination type 2 means that there are at least two elements in the password.
- Combination type 3 means that there are at least three elements in a password.
- Combination type 4 means that all four elements must be included in the password.

When the user sets the password, the system will check whether the password set meets the configuration requirements. Only the password that meets the requirements can be set successfully.

1. The password cannot be the same as the user name. When setting the administrator user password, if the password entered is the same as the user name, the system will not allow the password to be set.

Force to modify password for initial login:

When the function of "Force to modify the password when the user logs in for the first time" is enabled, when user first logs into the device, the system will output corresponding prompt information to ask the user to modify the password. Otherwise, the user is not allowed to log into the device. When the administrator's user name is "admin", whether or not the function of "Force to modify the password when the user logs in for the first time" is enabled, the user will be forced to modify the password when logging into the device for the first time.

Password lifetime:

Password lifetime is used to limit the using time of the user password. When the password is used longer than the password lifetime, the user needs to change the password. When a user logs in, and if the user enters an expired password, the system will prompt the user that the password has expired, and the password must be reset before local login. If the password entered does not meet the requirements, or if the new passwords entered twice are inconsistent, the system will refuse this login. For the non-interactive mode of login, such as FTP users, after the password lifetime expires, the user can log in only after the administrator modifies the password of FTP users; but if the password expires during the login period, it will not affect the operation of this login, but the next FTP command will trigger offline. In particular, if it is required to change the password for the first login, the password in fact has reached the expiration time, and the login will only require a unified password change once.

Maximum try times of the password:

The maximum try times of the user can be used to prevent malicious users from trying to decrypt the code. When the password try fails more than the maximum try times, the system will blacklist the user in the login-security module, and the user's account will be locked for a period of time.

Configuration Conditions

None

Configure Password Policy

Table 13-10 Configure the password policy

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-

Step	Command	Description
Configure the complexity of the password	**password-control complexity** {**min-length** *len*| **with user-name-check** | **composition type-number** *type-number* }	Optional By default, the minimum length of the user password is 6, the combination type of the password elements contains two kinds, and does not permit the user name to be the same as the password.
Configure forcing to modify the password when the user logs in for the first time	**password-control firstmodify enable**	Optional By default, do not force the user to modify the password when the user logs in for the first time. When the user named “admin” does not enable the command, it is also required to modify the password when logging in for the first time.
Configure the live time of the user	**password-control livetime** *user-live-time*	Optional By default, do not limit the live time of the user.
Configure the maximum times of the successive login authentication failure of the administrator user	**password-control max-try-time** *max-try-time-number*	Optional The command is configured in the administrator user group and administrator user. By default, the successive login authentication failure of the user in the administrator user group is not configured, that is, take the maximum times of the successive login authentication failure configured in the administrator user view as the main.

13.2.7. LUM Monitoring and Maintaining

Table 13-11 LUM monitoring and maintaining

Command	Description
debug user { manager | network}	Enable the debug information of the user management
show users class {manager | network}[*username*]	Display the configuration information of the user
show role [*rolename* **]**	Display the configuration information of all roles or specified role

13.3. LUM Typical Configuration Example

13.3.1. Configure Network Administrator User

Network Requirement

- Configure the network administrator user, and verify whether it has the network administrator authority.

Network Topology

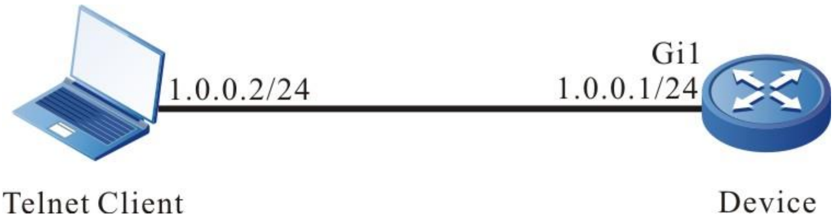


Figure 13-1 Networking for configuring the network administrator user group

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: Configure the administrator attributes.

#Configure the user as admin1 and password as admin2.

```
Device#configure terminal
Device(config)#local-user admin1 class manager
Device(config-user-manager-admin)#password 0 admin2
```

#Configure the service type.

```
Device(config-user-manager-admin1)#service-type telnet ftp web console ssh
```

#Configure the role of the local user as the network administrator.

```
Device(config-user-manager-admin1)#user-role network-admin
```

#Configure the local authorization, making the role take effect.

```
Device(config-user-manager-admin1)#exit
Device(config)#domain system
Device(config-isp-system)#aaa authentication login local
Device(config-isp-system)#aaa authorization login local
Device(config-isp-system)#exit
```

#Configure using the login aaa authentication in line vty.

```
Device(config)#line vty 0 15
Device(config-line)#login aaa
```

Step 3: At the Telnet client, input the user name admin1 and password admin2, and log into the device successfully.

#View whether the administrator user can execute the administrator command **show logging** to view the logs.

```
Device#show logging
Logging source configurations
  console is enabled,level: 7(debugging)
  monitor is enabled,level: 7(debugging)
  buffer is enabled,level: 5(notifications)
  file is enabled,level: 7(debugging)
The Context of logging file:
```

#Verify that the network administrator cannot execute the commands of other administrators.

```
Device#show role
You may not be authorized to perform this operation,please check.
```

Note:

- The default roles of the administrator have security-admin, network-operator, audit-admin, and network-admin. You can set the administrator role according to the demand, and also can the customized role.

14. ZTP

14.1. Overview

ZTP (zero touch provisioning) refers to the function of automatically loading version files (including system software, configuration files, license files, patch files, and customized files) when the new factory or empty configuration device is powered on and started.

The purpose is to solve the problem that when the network equipment is deployed, the administrator needs to go to the installation site to debug the software of the equipment after the hardware installation of the equipment is completed. When the number of devices is large and the distribution is wide, administrators need to manually configure each device, which not only affects the efficiency of deployment, but also requires high labor costs. With ZTP function, the device can obtain the version file from U disk or file server and load it automatically, so as to realize the device free of on-site configuration and deployment, so as to reduce the labor cost and improve the deployment efficiency.

ZTP is not a standard protocol, but a zero-configuration solution of equipment proposed by various manufacturers according to the market demand. There are differences in the implementation details, but the basic process is consistent. ZTP has many ways to start. Qtech currently supports DHCP zero-configuration starting, USB zero-configuration starting, and email starting. The process is that after the device enables the ZTP function, the empty configuration starting automatically enters the ZTP process. First, try to complete the auto opening through the inserted U disk. If the U-disk opening fails, try to complete the auto opening through DHCP.

The typical networking of DHCP zero-configuration starting is shown in Figure 14-1. When the null-configuration device enters the DHCP zero-configuration starting process, it will first broadcast the DHCP discovery packet through the DHCP client. If the DHCP server and the zero-configuration starting device are not in the same network segment, it needs to configure the DHCP relay to send the DHCP discovery message across network segments. When the DHCP server receives the DHCP discovery packet, it will assign the temporary IP address, default gateway and other information. At the same time, the intermediate file server address is returned. Then the DHCP client receives the response packet from the DHCP server, parses the address of the intermediate file server and other information, and downloads the intermediate file through FTP/TFTP/SFTP. Qtech currently supports the intermediate file of the XML format. Finally, analyze the intermediate file, download and upgrade the corresponding version and configuration from the intermediate file server according to the SN (serial number) of the device, and restart the device to take effect.

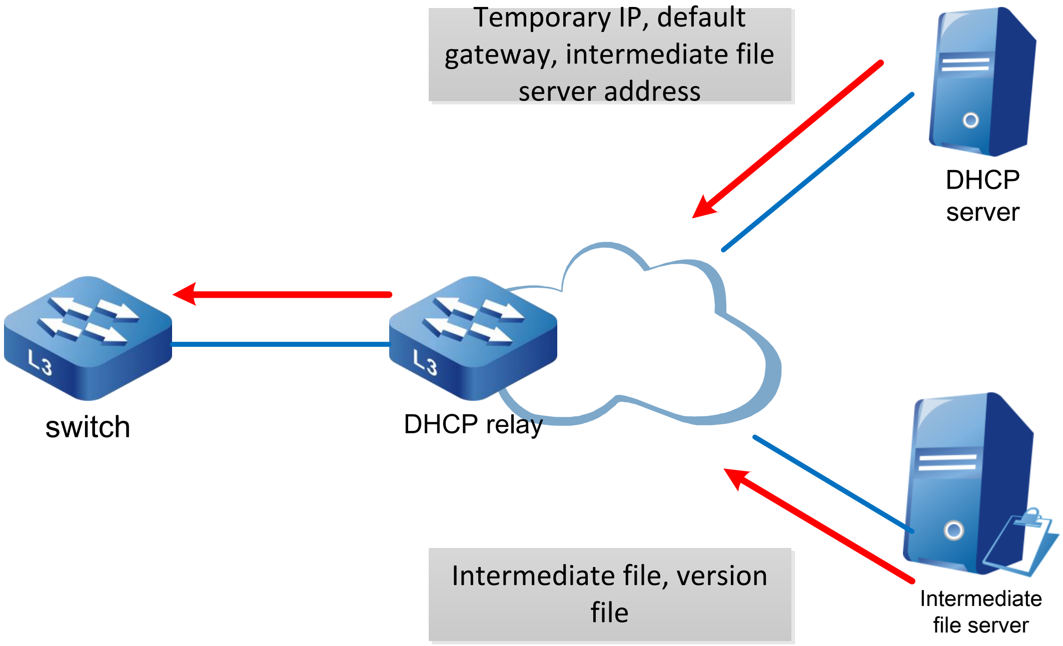

Temporary IP, default gateway, intermediate file server address
DHCP server
switch
DHCP relay
Intermediate file, version file
Intermediate file server

Figure 14-1DHCP typical networking

DHCP server: It is used to assign temporary management IP address, default gateway, intermediate file server address and other information to the device executing ZTP.

DHCP relay: when the device executing ZTP and the DHCP server are located in different network segments, it is necessary to forward the DHCP interactive packet through the DHCP relay.

Intermediate file server: It is used to save the intermediate files (the type of intermediate file is XML format), version files and configuration files needed by the device in ZTP process. The device executing ZTP can obtain the file server address, the corresponding version file and configuration file storage path and other information by parsing the intermediate file. The intermediate file server supports TFTP, FTP and SFTP.

Version file server: used to save the version files needed by the device, such as system software and configuration files. Version file server and intermediate file server can be deployed on the same file server, and support three types of TFTP, FTP and SFTP.

USB zero-configuration starting process: users edit the intermediate file, system version, configuration file and other information in advance and save them to USB, and then insert USB into the device to be zero-configuration started. When the device is powered on and detects the USB with the intermediate file meeting the conditions, it will enter the USB zero-configuration starting process, traverse the intermediate file according to the SN of the device, copy the corresponding system version and configuration file from USB, and then restart the device to take effect.

The typical networking of mail opening is shown in Figure 14-2 below. After the technical service personnel arrive at the customer's site, they first check the SN of the opening device, plug in the network cable and power on the device, and then notify the network management personnel of the SN. The network management personnel will edit the configuration file of the corresponding device in advance and deploy it to the file server. At the same time, they will make the corresponding URL and send it to the technical service personnel through the email server. Finally, the technical service personnel connect the device and enter the URL in the browser. After the customer clicks **Enter**, the webserver in the device will receive the message and start to parse the URL. According to the format specified in advance, the webserver will parse the file server address, configuration file path and other information from the URL, and download the configuration file to complete the mail starting.

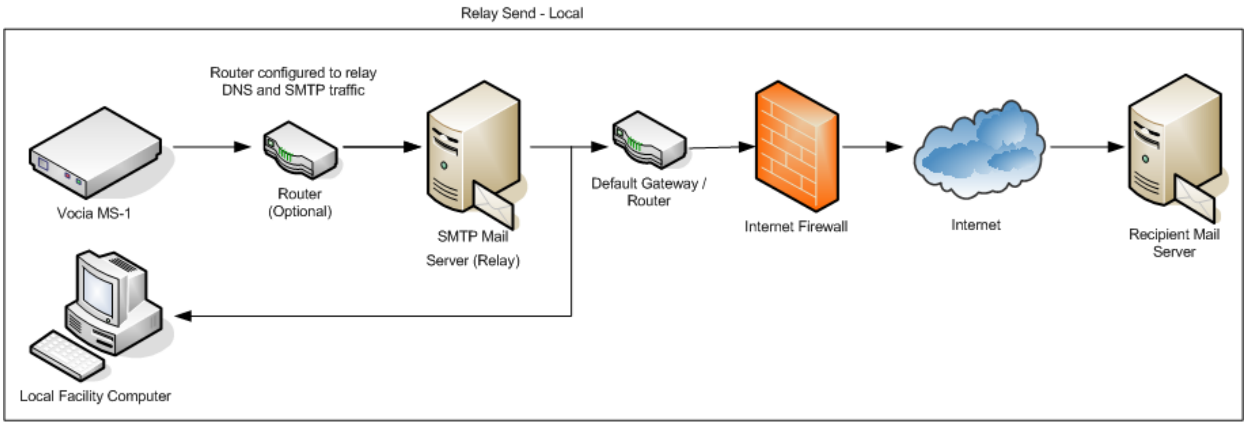


Figure 14-2 Typical networking of email opening

14.2. ZTP Function Configuration

14.2.1. Enable or Disable ZTP Function

Table 14-1 Enable or disable the ZTP function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the ZTP function	**ztp enable**	By default, the device does not enable the ZTP function.
Disable the ZTP function	**no ztp enable**	-

14.2.2. ZTP Monitoring and Maintaining

Table 14-2 ZTP monitoring and maintaining

Command	Description
show ztp	Display the ZTP information
[no] debug ztp	Enable or disable the ZTP debugging

14.3. ZTP Typical Configuration Example

14.3.1. Configure ZTP to Use Common Intermediate Files for Zero-configuration Deployment via DHCP

Network Requirement

- The PC, as the Console control terminal, is used to monitor the ZTP startup process of the device.
- As a DHCP server, Device2 provides the DHCP service for ZTP startup process.
- As a file server, Server1 provides FTP services (or SFTP, TFTP services) required by ZTP startup process.
- As a log server, Server2 receives the log information generated during ZTP startup.

Network Topology

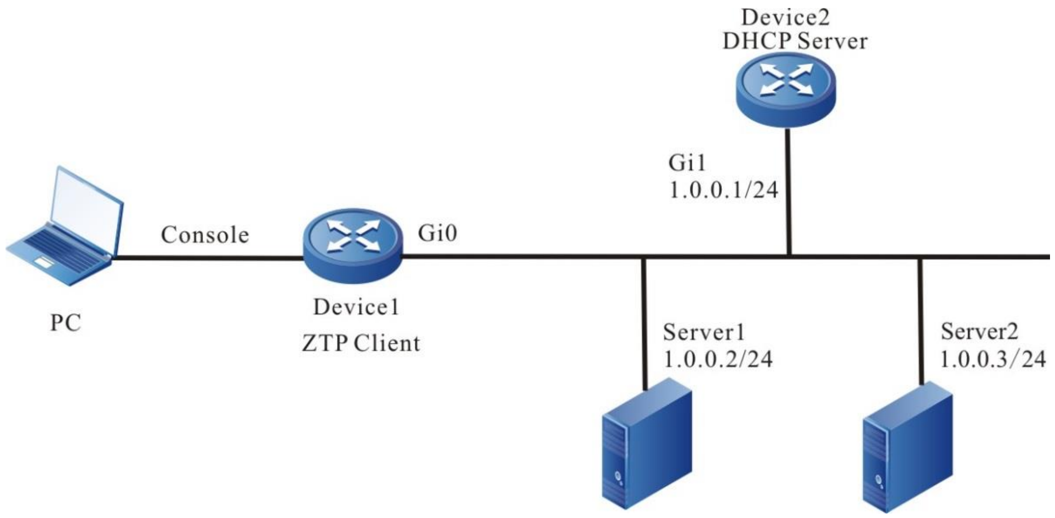


Figure 14-3 Networking for configuring the device to use the common intermediate file for zero-configuration deployment via DHCP

Configuration Steps

Step 1: To configure the FTP server, you will need to place the version files of the intermediate files (such as ztp.xml) and device configuration file to be downloaded in the directory of FTP server. (omitted)

#The method of editing ordinary intermediate files is as follows:

Right click to open editing in Excel mode

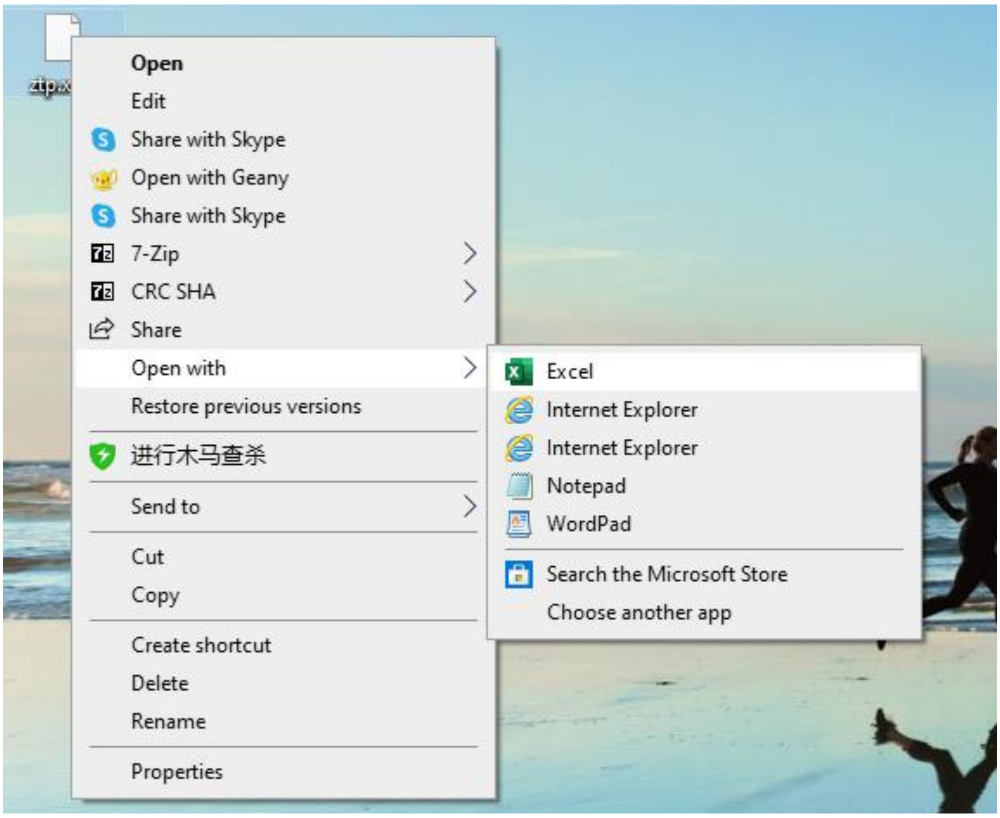
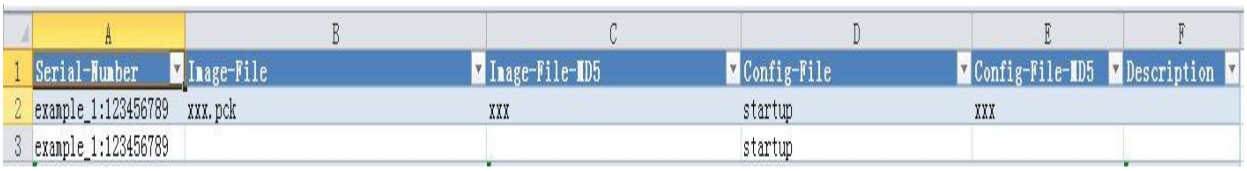


Figure 14-4 Open XML file graph with Excel to edit

Select as the XML table, and click OK.

You can edit it in Excel. Fill in the device serial number, version file name, version file name, MD5 check value, configuration file name, configuration file MD5 verification sum description information, and finally save it. Note that saving is in XML mode.



	A	B	C	D	E	F
1	Serial-Number	Image-File	Image-File-MD5	Config-File	Config-File-MD5	Description
2	example_1:123456789	xxx.pck	xxx	startup	xxx	
3	example_1:123456789			startup		

Figure 14-5 Edit the version and configuration file name in the XML file

Step 2: Enable the ZTP function of Device1.

```
Device1#configure terminal
Device1(config)#ztp enable
```

Step 3: Configure the DHCP service of Device2.

```
Device2#configure terminal
Device2(config)#ip dhcp pool ztp
Device2 (dhcp-config)#range 1.0.0.4 1.0.0.10 255.255.255.0
```

#Configure the intermediate file name option.

```
Device2 (dhcp-config)#option 67 ascii ztp.xml
```

#Configure the file download method and server address, user name and password options

```
Device2 (dhcp-config)#option 66 ascii ftp://[a[:a]@]1.0.0.2
```

#Configure the log server address option.

```
Device2 (dhcp-config)#option 7 ip 1.0.0.3
Device2 (dhcp-config)#exit
```

#The server enables the DHCP service.

```
Device2(config)#interface gigabitethernet1
Device2(config-if-gigabitethernet1)#ip address 1.0.0.1/24
Device2(config-if-gigabitethernet1)#ip dhcp server
Device2(config-if-gigabitethernet1)#end
```

Step 4: Device1 starts with empty configuration, enters ZTP process, downloads version upgrade and loads configuration file.

#Through the following log, you can see that the device enters the ZTP process, and sends the DHCP request.

```
May  6 2020 15:04:19 Device1 MPU0 %ZTP-5:Now starting DHCP upgrade...
May  6 2020 15:04:19 Device1 MPU0 %ZTP-5:DHCP discovery phase started...
```

#During the ZTP request period, you can exit the ZTP process through Ctrl + C, so that the null configuration can be started. If you do not press Ctrl + C, you can continue to follow the ZTP process.

```
May  6 2020 15:04:23 Device1MPU0 %ZTP-5:Press (ctrl + c) to abort Dhcp Upgrade
```

#Get the address successful, and download the common intermediate file.

```
May  6 2020 15:06:29 Device1 MPU0 %DHCP-ASSIGNED_EXT-5:Interface gigabitethernet0 assigned DHCP address 1.0.0.4, mask 255.255.255.0.
May  6 2020 15:06:31 Device1 MPU0 %ZTP-5:Dhcp Upgrade DHCP discovery phase success
May  6 2020 15:06:31 Device1 MPU0 %ZTP-5:Start to download temp file ztp.xml
```

#Analyze the intermediate file, and download the version information.

```
May  6 2020 15:06:56 Device1 MPU0 %ZTP-5:Download temp file ztp.xml is success
May  6 2020 15:06:56 Device1 MPU0 %ZTP-5:Start to parse temp file...
May  6 2020 15:06:56 Device1 MPU0 %ZTP-5:parse temp file is success
May  6 2020 15:06:56 Device1 MPU0 %ZTP-5:Start to download the Image file ztp.pck
```

#Download the version and configuration file successfully, and then restart the device automatically through ZTP.

```
May  6 2020 15:14:09 Device1 MPU0 %SYS_UPDATE-RESULT-5:image : Mpu 0 upgrade successfully!
May  6 2020 15:14:11 Device1 MPU0 %ZTP-5:Download the Image file is success
May  6 2020 15:14:11 Device1 MPU0 %ZTP-5:Start to download the config file startup_ztp...
May  6 2020 15:14:12 Device1 MPU0 %ZTP-5:Download the config file is success
May  6 2020 15:14:12 Device1 MPU0 %ZTP-5:DHCP upgrade is success
May  6 2020 15:14:12 Device1 MPU0 %ZTP-5:System will rebooted by DHCP upgrade
```

Step 5: Check the result.

Check the ZTP status through show ztp, execute the commands **show running config** and **show version**, and you can see that the configuration and version take effect.

```
Device1#show ztp


Last ztp method: DHCP upgrade method
   Ztp state: ZTP DHCP upgrade success
   Ztp important inforamtion:
      FTP server IP: 1.0.0.2
      Temporary file name: ztp.xml
      Startup file name:startup_ztp
      Image file name:ztp.pck


Current ztp method: None upgrade method
```

14.3.2. ZTP to Use Common Intermediate Files for Zero-configuration Deployment via USB

Network Requirement

- The PC, as the Console control terminal, is used to monitor the ZTP startup process of the device.
- Device1 is inserted into the USB device. The USB device contains intermediate file, version file, and device configuration file.

Network Topology

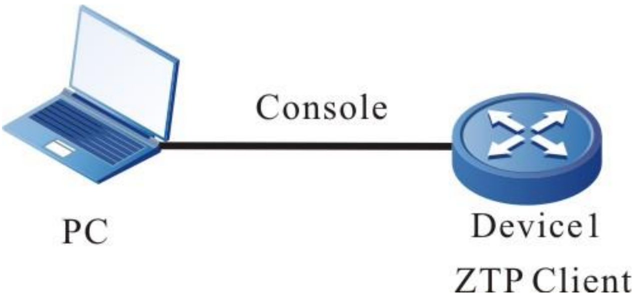


Figure 14-6 Networking for configuring the device to use the common intermediate file for zero-configuration deployment via DHCP

Configuration Steps

Step 1: Place the intermediate file in the USB root directory, and name as ztp_config.xml, that is /usb/ztp_config.xml.

#The method of editing the common intermediate file is as follows:

Right-click, and open by Excel to edit.

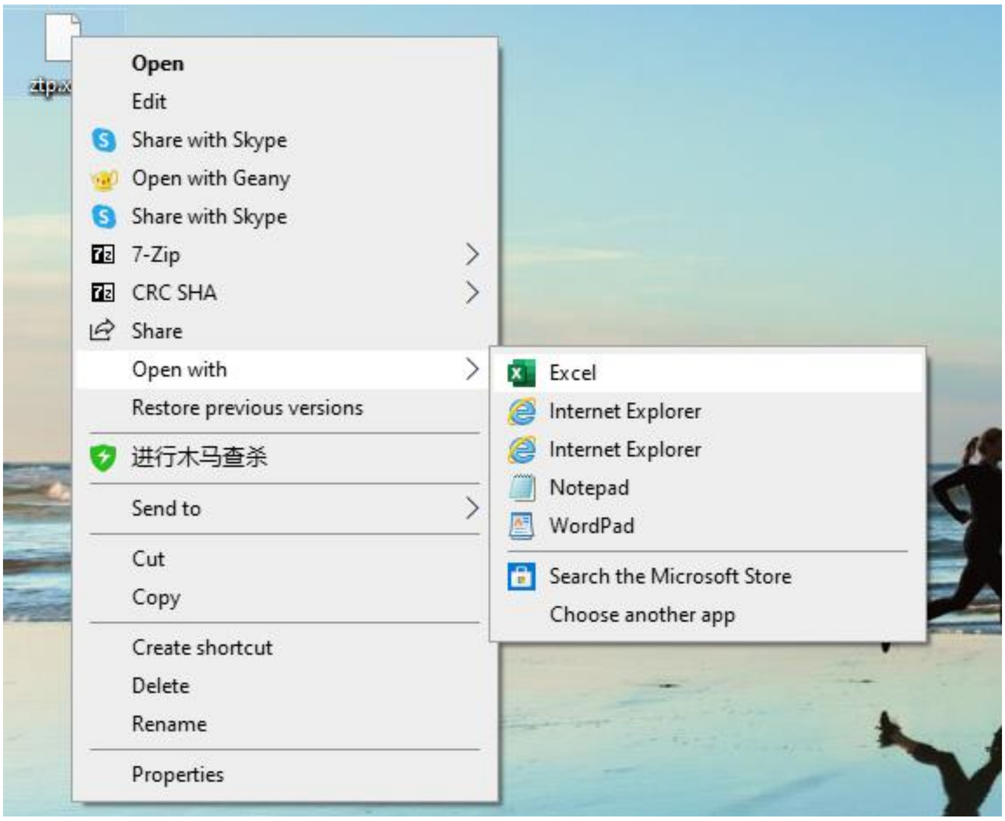
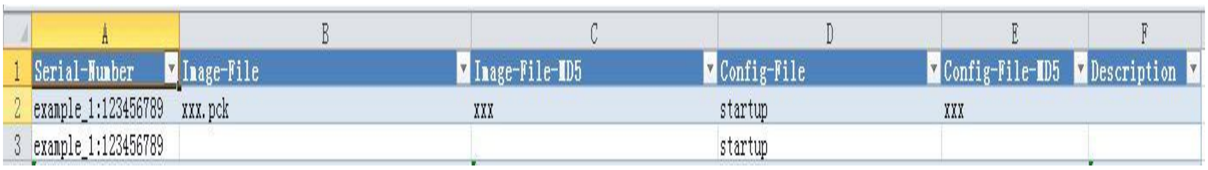


Figure 14-7 Open XML file graph with Excel to edit

Select as the XML table, and click OK.

You can edit it in Excel. Fill in the device serial number, version file name, version file name, MD5 check value, configuration file name, configuration file MD5 verification sum description information, and finally save it. Note that saving is in XML mode.



	A	B	C	D	E	F
1	Serial-Number	Image-File	Image-File-MD5	Config-File	Config-File-MD5	Description
2	example_1:123456789	xxx.pck	xxx	startup	xxx	
3	example_1:123456789			startup		

Figure 14-8 Edit the version and configuration file name in the XML file

<u>Note:</u>

- XXX is the corresponding IOS version name in USB.
- The XML intermediate file is obtained from the ZTP path of the software release manual.
- In XML intermediate file, the required fields are serial number, version and configuration file, and serial number can be obtained from the equipment delivery list; the version name

and configuration file name filled in the XML intermediate file must be consistent with the IOS version file name and configuration file name in USB. Otherwise, the opening fails.

- MD5 code, MD5 code of configuration file, and description information in XML intermediate file are optional. If MD5 code is required, it can be generated by general MD5 code calculation tool.

Step 2: Put the version file and configuration file corresponding to the device serial number in the intermediate file into the USB root directory, and the name is consistent with the description of the intermediate file. (omitted)

Step 3: Enable the ZTP function of Device1.

```
Device1#configure terminal

Device1(config)#ztp enable
```

Step 4: Power on the device, enter the ztp process, and perform the deployment by USB.

```
#The device configuration is empty, and enter the USB deployment process.

the current config file /flash/startup does not exist.

The backup file /backupramfs/startup is not exist.

The current config file /backup/startup does not exist.

May  6 2020 15:16:15 Device1MPU0 %ZTP-USB_UPGRADE-5:Now starting USB upgrade...

#Search and analyze the intermediate file.

May  6 2020 15:16:15 Device1MPU0 %ZTP-USB_UPGRADE-5:Start to copy the temporary file /usb/ztp_config.xml...

May  6 2020 15:16:15 Device1MPU0 %ZTP-USB_UPGRADE-5:Copy the temporary file is success.

May  6 2020 15:16:15 Device1MPU0 %ZTP-USB_UPGRADE-5:Start to parse the temporary file /flash/ztp_config.xml

#Upgrade the version and configuration.

May  6 2020 15:16:15 Device1MPU0 %ZTP-USB_UPGRADE-5:Parse temporary file is success

May  6 2020 15:19:53 Device1MPU0 %ZTP-USB_UPGRADE-5:Sysupdate image is success

May  6 2020 15:19:53 Device1 MPU0 %ZTP-USB_UPGRADE-5:Start to copy config...

May  6 2020 15:19:54 Device1  MPU0 %ZTP-USB_UPGRADE-5:Copy config is success

#Restart after upgrading.

May  6 2020 15:19:54 Device1 MPU0 %ZTP-USB_UPGRADE-4:System will be rebooted by USB Upgrade
```

Step 5: Check the result.

#Check the ZTP status via the command **show ztp**. Execute the commands **show running-config** and **show version**, and you can see that the configuration and version take effect.

```
Device1#show ztp


Last ztp method: USB upgrade method
   Ztp state: ZTP USB Upgrade success
   Ztp important information:
      Temporary file name:/usb/ztp_config.xml
      Startup file name:startup
      Image file name:ztp.pck


Current ztp method: None upgrade method


Next ztp state: disable
```

Note:

- If the general intermediate file version information is empty, then the ZTP process of the device will not upgrade the version, but only load the configuration and continue the ZTP process, but the configuration file cannot be empty.
- The device will copy and download the version and configuration file from USB, so it is necessary to put the version and configuration file into USB.
- The name of ordinary intermediate file in USB can only be ZTP_ config.xml.

14.3.3. Zero-Configuration Opening via Mail

Network Requirements

- Device is the opened device, and the routes between the devices are interworking.
- The controller is responsible for sending the opening email to the PC and acting as the FTP server.
- PC is used to receive the opening e-mail, start the e-mail on the device, and monitor the starting process of the e-mail on the device.
- The mail server is responsible for managing the sending and receiving of mail.

Network Topology

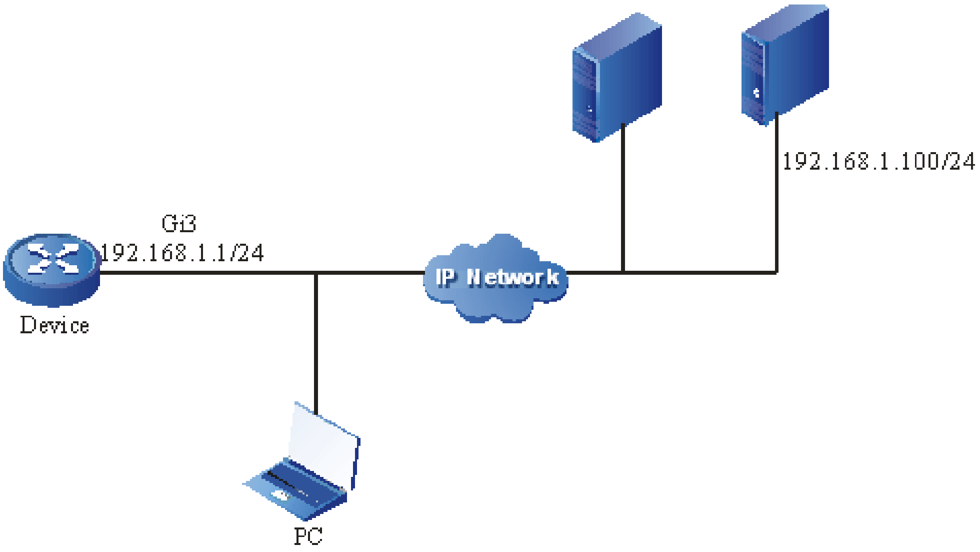


Figure 14-9 Networking for configuring zero-configuration opening via mail

Configuration Steps

Step 1: On the controller, click Resource Zero-configuration opening Template Template management Add configuration template. The template content is device configuration.

Note:

- Please read the instructions and examples when adding template content.

Step 2: Click **Template** > **Download excel file of parameter table**, open the parameter table and fill in equipment information, and import the parameter table.

#The content of the parameter table:

#Import the parameter table:

Note:

- xxx is the corresponding device name, and yyy is the corresponding device model.
- The serial number can be found in the factory list of the equipment.

Step 3: Select the device to be started on the controller and click **Configuration Loading Mail loading**. After setting the opening configuration and recipient, click **OK** to send the mail.

Step 4: After receiving the email on PC, open the link and click the **Starting** button to start the device via mail. After starting successfully, the device will restart automatically.

#Download the configuration:

```
Device#
Oct 20 2020 17:41:41 Device MPU0 %WEB-MAIL-UPD-5:SerialNum:123456789 Version:1,
parse upgrade-config successfully.
Oct 20 2020 17:41:41 Device MPU0 %WEB-MAIL-UPD-5:SerialNum:123456789 Version:1,
downloading remote config-file.
Oct 20 2020 17:41:41 Device MPU0 %WEB-MAIL-UPD-5:SerialNum:123456789 Version:1,
download remote config-file successfully.
Oct 20 2020 17:41:41 Device MPU0 %WEB-MAIL-UPD-5:SerialNum:123456789 Version:1,
validating remote config-file.
Please wait...system reloading is in progress!
```

#After downloading successfully, check whether the configuration file is legal, and restart the device after it is legal:

```
Reset system!
Oct 20 2020 17:41:45 Device MPU0 %WEB-MAIL-UPD-5:SerialNum:123456789 Version:1,
remote config-file valid.
Oct 20 2020 17:41:45 Device MPU0 %WEB-MAIL-UPD-5:SerialNum:123456789 Version:1,
executing remote config-file.
Oct 20 2020 17:41:45 Device MPU0 %WEB-MAIL-UPD-5:SerialNum:123456789 Version:1,
execue remote config-file successfully.
Oct 20 2020 17:41:45 Device MPU0 %WEB-MAIL-UPD-5:SerialNum:123456789 Version:1,
update successfully, device is about to restart.
```

Step 5: Check the result.

. #After the device is restarted, check whether the device configuration is consistent with the opening configuration

Note:

- In the process of mail opening, it is necessary to ensure that the serial number of the device is consistent with that of the device.
- The length of URL allowed by each browser is different. It is recommended that the initial configuration length should not exceed 5000 bytes.
- The content of the template involving the password needs to be changed to plaintext.
- If the factory configuration does not complete the configuration of managing address and enabling web service, the administrator needs to configure managing address and enabling web service.

15. ОБЩАЯ ИНФОРМАЦИЯ

15.1. Замечания и предложения

Мы всегда стремимся улучшить нашу документацию и помочь вам работать лучше, поэтому мы хотим услышать вас. Мы всегда рады обратной связи, в особенности:

- ошибки в содержании, непонятные или противоречащие места в тексте;
- идеи по улучшению документации, чтобы находить информацию быстрее;
- неработающие ссылки и замечания к навигации по документу.

Если вы хотите написать нам по поводу данного документа, то используйте, пожалуйста, форму обратной связи на qtech.ru.

15.2. Гарантия и сервис

Процедура и необходимые действия по вопросам гарантии описаны на сайте QTECH в разделе «Поддержка» −> «Гарантийное обслуживание».

Ознакомиться с информацией по вопросам тестирования оборудования можно на сайте QTECH в разделе «Поддержка» −> «Взять оборудование на тест».

Вы можете написать напрямую в службу сервиса по электронной почте sc@qtech.ru.

15.3. Техническая поддержка

Если вам необходимо содействие в вопросах, касающихся нашего оборудования, то можете воспользоваться нашей автоматизированной системой запросов технического сервис-центра helpdesk.qtech.ru.

Телефон Технической поддержки +7 (495) 797-33-11 доб. 0