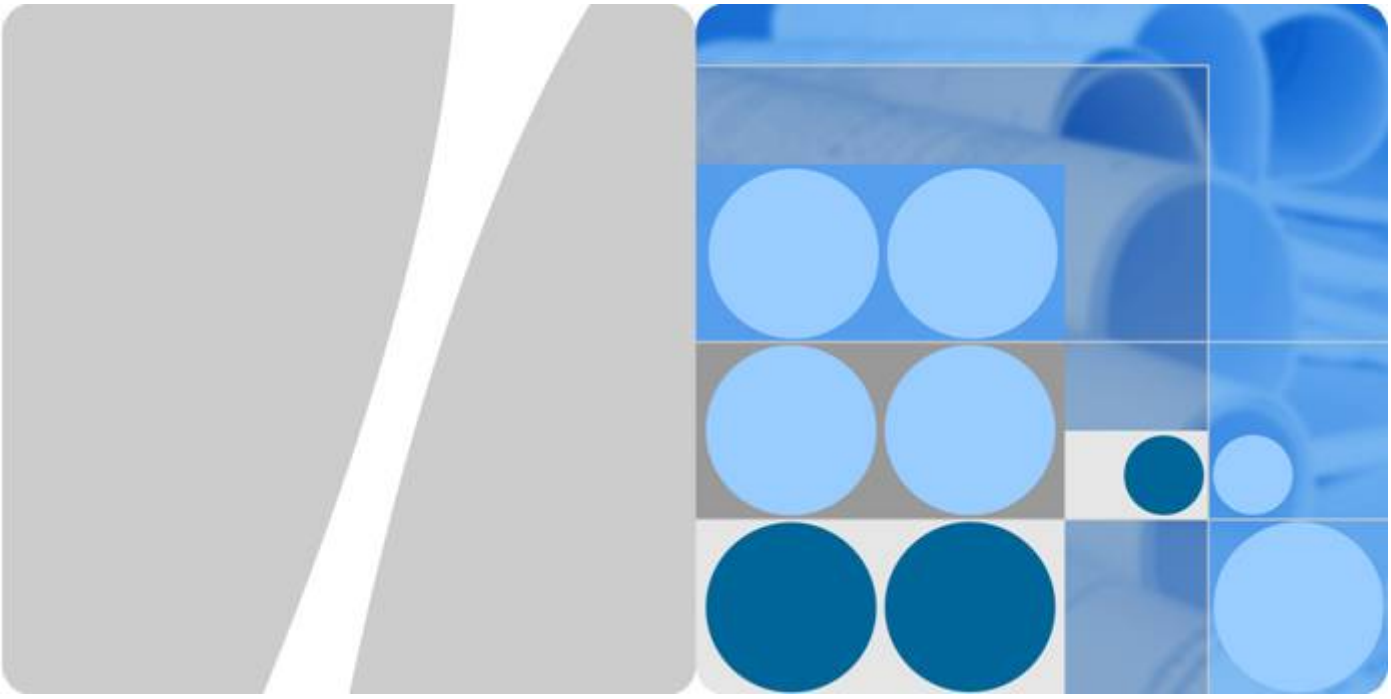


Huawei AR Series Access Routers

V200R010

CLI-based Configuration Guide - Basic Configuration

Issue 14

Date 2024-08-30

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://e.huawei.com

About This Document

Intended Audience

This document provides the basic concepts, configuration procedures, and configuration examples in different application scenarios of the Basic configuration supported by the device.

This document is intended for:

- Data configuration engineers
- Commissioning engineers
- Network monitoring engineers
- System maintenance engineers

Symbol Conventions

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

Symbol	Description
	Indicates a hazard with a high level of risk which, if not avoided, will result in death or serious injury.
	Indicates a hazard with a medium level of risk which, if not avoided, could result in death or serious injury.
	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.
	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.

 Copyright © Huawei Technologies Co., Ltd.

Symbol	Description
NOTE	Supplements the important information in the main text. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Command Conventions

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

Convention	Description
Boldface	The keywords of a command line are in **boldface**.
Italic	Command arguments are in *italics*.
[ ]	Items (keywords or arguments) in brackets [ ] are optional.
{ x | y | ... }	Optional items are grouped in braces and separated by vertical bars. One item is selected.
[x | y | ...]	Optional items are grouped in brackets and separated by vertical bars. One item is selected or no item is selected.
{ x | y | ... }*	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[x | y | ...]*	Optional items are grouped in brackets and separated by vertical bars. Several items or no item can be selected.
&<1-n>	The parameter before the & sign can be repeated 1 to n times.
#	A line starting with the # sign is comments.

Interface Numbering Conventions

Interface numbers used in this manual are examples. In device configuration, use the existing interface numbers on devices.

 Copyright © Huawei Technologies Co., Ltd.

Security Conventions

- Password setting
  - When configuring a password, the cipher text is recommended. To ensure device security, change the password periodically.
  - When you configure a password in plain text that starts and ends with %@%@, @%@%, %#%#, or %^%# (the password can be decrypted by the device), the password is displayed in the same manner as the configured one in the configuration file. Do not use this setting.
  - When you configure a password in cipher text, different features cannot use the same cipher-text password. For example, the cipher-text password set for the AAA feature cannot be used for other features.
- Encryption algorithm

  Currently, the device uses the following encryption algorithms: 3DES, AES, RSA, SHA1, SHA2, and MD5. 3DES, RSA and AES are reversible, while SHA1, SHA2, and MD5 are irreversible. The encryption algorithms DES, 3DES, RSA (RSA-1024 or lower), MD5 (in digital signature scenarios and password encryption), and SHA1 (in digital signature scenarios) have a low security, which may bring security risks. If protocols allowed, using more secure encryption algorithms, such as AES, RSA (RSA-2048 or higher), SHA2, and HMAC-SHA2, is recommended. The encryption algorithm depends on actual networking. The irreversible encryption algorithm must be used for the administrator password, SHA2 is recommended.
- Personal data

  Some personal data may be obtained or used during operation or fault location of your purchased products, services, features, so you have an obligation to make privacy policies and take measures according to the applicable law of the country to protect personal data.
- The terms mirrored port, port mirroring, traffic mirroring, and mirroring in this manual are mentioned only to describe the product's function of communication error or failure detection, and do not involve collection or processing of any personal information or communication data of users.

Reference Standards and Protocols

To obtain reference standards and protocols, log in to **Huawei official website**, search for "protocol compliance list", and download the *Huawei AR Series Standard and Protocol Comply Table*.

Declaration

- This manual is only a reference for you to configure your devices. The contents in the manual, such as web pages, command line syntax, and command outputs, are based on the device conditions in the lab. The manual provides instructions for general scenarios, but do not cover all usage scenarios of all product models. The contents in the manual may be different from your actual device situations due to the differences in software versions, models, and configuration files. The manual will not list every possible difference. You should configure your devices according to actual situations.

 Copyright © Huawei Technologies Co., Ltd.

- The specifications provided in this manual are tested in lab environment (for example, the tested device has been installed with a certain type of boards or only one protocol is run on the device). Results may differ from the listed specifications when you attempt to obtain the maximum values with multiple functions enabled on the device.
- In this document, public IP addresses may be used in feature introduction and configuration examples and are for reference only unless otherwise specified.
- In this document, AR series access routers include AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600 Series.

Mappings Between Product Software Versions and NMS Versions

The mappings between product software versions and NMS versions are as follows.

AR Product Software Version	eSight	iManager U2000
V200R010	V300R009C00	V200R018C50

 Copyright © Huawei Technologies Co., Ltd.

Contents

About This Document ii

1 Overview of CLIs 1

1.1 Licensing Requirements and Limitations for CLIs 1
1.2 How to Use Command Lines 2
1.2.1 Entering Command Views 2
1.2.2 Setting Command Levels 4
1.2.3 Editing Command Lines 5
1.2.4 Using Command Line Online Help 7
1.2.5 Interpreting Command Line Error Messages 9
1.2.6 Using the **undo** Command Line 9
1.2.7 Displaying History Commands 10
1.2.8 Using Command Line Shortcut Keys 11
1.2.9 Executing Commands in a Batch 13
1.3 Displaying the Command Output 14
1.3.1 Verifying Command Line Configurations 14
1.3.2 Configuring Users of Different Levels to View Different Configurations 15
1.3.3 Controlling the Display Mode of Commands 15
1.3.4 Filtering Command Outputs 16
1.4 FAQ of CLIs 20
1.4.1 What Are Shortcut Keys ESC_B and ESC_F For? 20
1.4.2 How Do I Define the Command Level? 20

2 Auto-Config Configuration 21

2.1 Overview of Auto-Config 22
2.2 Understanding Auto-Config 22
2.2.1 Auto-Config Fundamentals 22
2.2.2 Working Process of Auto-Config 23
2.2.3 Option Parameters 26
2.2.4 Intermediate File 30
2.3 Application Scenarios for Auto-Config 30
2.4 Licensing Requirements and Limitations for Auto-Config 32
2.5 Default Settings for Auto-Config 33
2.6 Configuring Auto-Config on Devices that are on the Same Network Segment with the DHCP Server 34

 Copyright © Huawei Technologies Co., Ltd.

2.6.1 Enabling Auto-Config....34
2.6.2 (Optional) Configuring the Intermediate File....35
2.6.3 Configuring the DHCP Server....36
2.6.4 Configuring the File Server....40
2.6.5 Powering on the Device to Start Auto-Config....41
2.6.6 Verifying the Configuration....41
2.7 Configuring Auto-Config Across Different Network Segments....41
2.7.1 Enabling Auto-Config....42
2.7.2 (Optional) Configuring the Intermediate File....43
2.7.3 Configuring the DHCP Server....44
2.7.4 Configuring the DHCP Relay Function....48
2.7.5 Configuring the File Server....49
2.7.6 Powering on the Device to Start Auto-Config....50
2.7.7 Verifying the Configuration....50
2.8 Maintaining Auto-Config....51
2.9 Configuration Examples for Auto-Config....52
2.9.1 Example for Configuring Auto-Config on the Same Network Segment....52
2.9.2 Example for Configuring Auto-Config on Different Network Segments....56

3 Auto-Start Configuration....61

3.1 Overview of Auto-Start....61
3.2 Application Scenarios for Auto-Start....62
3.3 Understanding Auto-Start....63
3.4 Licensing Requirements and Limitations for Auto-Start....66
3.5 Default Settings for Auto-Start....66
3.6 Configuring Auto-Start....66
3.6.1 Making the Intermediate File....67
3.6.2 Configuring the File Server....68
3.6.3 Configuring Auto-Start On a Device....69
3.7 Maintaining Auto-Start....70
3.8 Configuration Examples for Auto-Start....71
3.8.1 Example for Configuring Auto-Start....71

4 USB-based Deployment Configuration....76

4.1 Overview of USB-based Deployment....76
4.2 Understanding USB-based Deployment....77
4.3 Licensing Requirements and Limitations for USB-based Deployment....81
4.4 Making an Index File....81
4.5 Performing USB-based Deployment....96
4.6 Configuration Examples for USB-based Deployment....101
4.6.1 Example for Configuring USB-based Deployment....101

5 SMS-based Deployment Configuration....106

5.1 Overview of SMS-based deployment....106

 Copyright © Huawei Technologies Co., Ltd.

5.2 Understanding SMS-based Deployment 107
5.3 Application Scenarios for SMS-based Deployment 109
5.4 Licensing Requirements and Limitations for SMS-based Deployment 110
5.5 Default Settings for SMS-based Deployment 111
5.6 Configuring SMS-based Deployment 111
5.6.1 Configuring SMS-based Deployment 111
5.7 Configuration Examples for SMS-based Deployment 125
5.7.1 Example for Configuring SMS-based Deployment 125
6 Plug-and-Play Deployment Configuration 136
6.1 Overview of Plug-and-Play Deployment 136
6.2 Understanding Plug-and-Play Deployment 137
6.3 Application Scenarios for Plug-and-Play Deployment 142
6.4 Licensing Requirements and Limitations for Plug-and-Play Deployment 144
6.5 Configuring Plug-and-Play Deployment 145
7 Fast Provisioning Configuration 147
7.1 Overview of Fast Provisioning 147
7.2 Enabling the Fast Provisioning Function 151
7.3 Maintaining the Fast Provisioning Function 153
7.4 Licensing Requirements and Limitations for Fast Provisioning 154
7.5 Configuration Examples for Fast Provisioning 154
7.5.1 Example for Configuring the Fast Provisioning Function 154
8 First Login to a Device 157
8.1 Overview of the First Login 157
8.2 Licensing Requirements and Limitations for the First Login 158
8.3 Logging In to a Device 158
8.3.1 Logging In to a Device for the First Time Through a Console Port 158
8.3.2 Logging In to a Device for the First Time Through a Mini USB Port 162
8.4 Basic Configuration on a Device at the First Login (Console Port or Mini USB Port) 166
8.5 Configuration Examples for Logging In to a Device for the First Time 170
8.5.1 Example for Performing Basic Configuration on the Device at First Login 170
9 CLI Login Configuration 173
9.1 Overview of CLI Login Methods 174
9.2 Overview of User Interfaces 178
9.3 Licensing Requirements and Limitations for CLI Login 181
9.4 Configuring Login Through a Console Port 181
9.4.1 (Optional) Configuring Attributes for the Console User Interface 182
9.4.2 Configuring an Authentication Mode for the Console User Interface 184
9.4.3 Configuring a User Level for the Console User Interface 185
9.4.4 Logging In to a Device Through the Console Port 186
9.5 Configuring Login Through the Mini USB Port 190
9.5.1 (Optional) Configuring Attributes for the Console User Interface 190

 Copyright © Huawei Technologies Co., Ltd.

9.5.2 Configuring an Authentication Mode for the Console User Interface....192
9.5.3 Configuring a User Level for the Console User Interface....193
9.5.4 Logging In to a Device Through the Mini USB Port....194
9.6 Configuring Telnet Login....197
9.6.1 (Optional) Configuring Attributes for a VTY User Interface....197
9.6.2 Configuring an Authentication Mode for a VTY User Interface....198
9.6.3 Configuring a User Level for a VTY User Interface....200
9.6.4 Enabling the Telnet Server Function....201
9.6.5 Logging In to a Device Through Telnet....203
9.6.6 (Optional) Using Telnet to Log In to Another Device From the Local Device....204
9.7 Configuring STelnet Login....205
9.7.1 (Optional) Configuring Attributes for a VTY User Interface....205
9.7.2 Configuring an Authentication Mode for a VTY User Interface....207
9.7.3 Configuring a User Level for a VTY User Interface....208
9.7.4 Configuring an SSH User....209
9.7.5 Enabling the SSH Server Function....211
9.7.6 Logging In to a Device Through STelnet....214
9.7.7 (Optional) Using STelnet to Log In to Another Device from the Local Device....216
9.8 Configuring the Redirection Function for Device Login....219
9.8.1 (Optional) Configuring an Authentication Mode for TTY User Interface....219
9.8.2 Logging In to a Device Through Redirection....220
9.9 Configuring Reverse Telnet Login....225
9.9.1 Configuring an Authentication Mode for the Console or TTY User Interface....225
9.9.2 Logging In to a Device Through Reverse Telnet (Direct Connection Through an Asynchronous Cable)....226
9.9.3 Configuring Reverse Telnet Login (Direct Connection Through a Console Cable)....228
9.10 Typical Operations After Login....229
9.11 Configuration Examples for CLI Login....231
9.11.1 Example for Logging In to the Device Through a Console Port....231
9.11.2 Example for Configuring a Security Policy to Limit Telnet Login....233
9.11.3 Example for Logging In to the Device Through STelnet....235
9.11.4 Example for Configuring the Device as the Telnet Client to Log In to Another Device....246
9.11.5 Example for Configuring the Device as the STelnet Client to Log In to Another Device....248
9.11.6 Example for Logging In to Another Device Through Redirection....254
9.11.7 Example for Configuring an NMS to Communicate with a Device by SSH over a VPN....256
9.12 Troubleshooting CLI Login....261
9.12.1 Failing to Log In Through the Console Port....261
9.12.2 Failing to Log In Through Telnet....262
9.12.3 Failing to Log In Through STelnet....263
9.13 FAQ About CLI Login....265
9.13.1 What Is the Default Login Password?....265
9.13.2 What If I Forget the Password for Console Port Login?....265
9.13.3 What If I Forget the Password for Telnet Login?....266

9.13.4 How Do I Configure Screen Display? 267
9.13.5 How Do I Force an Online User to Go Offline? 267
9.13.6 What Are System Users of AR Routers? 268
10 Web System Login Configuration 271
10.1 Overview of Web System Login 272
10.2 Licensing Requirements and Limitations for Web System Login 272
10.3 Default Settings for Web System Login 273
10.4 Configuring Device Login Through the Web System 273
10.4.1 Configuring a Management IP Address for the Device 273
10.4.2 (Optional) Uploading and Loading the Web Page File 274
10.4.3 (Optional) Configuring Web System Parameters 275
10.4.4 (Optional) Setting the Storage Directory of the Logo Image on the Web Page 277
10.4.5 Creating a Web System Account 278
10.4.6 Logging In to the Web System 279
10.4.7 Verifying the Configuration 282
10.5 Configuration Examples for Web System Login 282
10.5.1 Example for Configuring Device Login Through the Web System 282
10.6 Common Misconfigurations 284
10.6.1 Device Login Through the Web System Fails 285
10.6.2 The Web System Page Is Not Completely Displayed After Successful Device Login Through the Web System 286
10.7 FAQ About Web System Login 287
10.7.1 Does the AR Series Support the Web NMS? 287
10.7.2 How Do I Configure the Web User Level? 287
10.7.3 What Should I Do If I Forget the Web System Login Password? 287
10.7.4 What Is the Default Login Password? 287
10.7.5 What Should I Do If the Account Is Locked? 288
10.7.6 How Do I Obtain the Web Page File? 288
10.7.7 How Do I Change the Port Number for Web System Login? 288
11 File Management 289
11.1 Overview of the File System 289
11.2 File Management Modes 291
11.3 Licensing Requirements and Limitations for File Management 293
11.4 Local File Management 293
11.4.1 Logging In to the Device to Manage Files 293
11.4.2 Managing Files When the Device Functions as a TFTP Server 296
11.4.3 Managing Files When the Device Functions as an FTP Server 299
11.4.4 Managing Files When the Device Functions as an SFTP Server 306
11.5 File Management on Other Devices 319
11.5.1 Managing Files When the Device Functions as a TFTP Client 319
11.5.2 Managing Files When the Device Functions as an FTP Client 322
11.5.3 Managing Files When the Device Functions as an SFTP Client 328

 Copyright © Huawei Technologies Co., Ltd.

11.6 Configuration Examples for File Management....335
11.6.1 Example of Logging In to the Device to Manage Files....335
11.6.2 Example for Managing Files When the Device Functions as a TFTP Server....336
11.6.3 Example for Managing Files When the Device Functions as an FTP Server....338
11.6.4 Example for Managing Files Using SFTP When the Device Functions as an SSH Server....340
11.6.5 Example for Managing Files When the Device Functions as a TFTP Client....343
11.6.6 Example for Managing Files When the Device Functions as an FTP Client....344
11.6.7 Example for Managing Files When the Device Functions as an SFTP Client....345
11.7 Troubleshooting System Startup....350
11.7.1 FTP Login Failure....350
11.7.2 Failure in Uploading Files to the FTP Server....352
11.8 FAQ About File Management....353
11.8.1 Does an AR Router Support Resumable FTP Download?....353
11.8.2 How Many FTP Users Can Log In to a Router Simultaneously?....353
11.8.3 Why Does the Available Space on a Storage Medium Not Change After a File Is Deleted?....354
12 Configuring System Startup....355
12.1 Overview of System Startup....356
12.2 Licensing Requirements and Limitations for System Startup....360
12.3 Managing Configuration Files....360
12.3.1 Saving the Configuration File....360
12.3.2 Comparing Configuration Files....362
12.3.3 Backing Up the Configuration File....363
12.3.4 Recovering the Configuration File....364
12.3.5 Clearing the Configuration File....366
12.3.6 Setting Factory Configurations....367
12.4 Configuring System Startup Files....369
12.5 Restarting the Device....371
12.6 Configuration Examples for System Startup....372
12.6.1 Example for Backing Up the Configuration File....372
12.6.2 Example for Recovering the Configuration File....373
12.6.3 Example of Configuring System Startup....374
13 BootROM Menu....378
13.1 Overview of the BootROM Menu....378
13.2 Licensing Requirements and Limitations for the BootROM Menu....379
13.3 BootROM Main Menu....379
13.4 Serial Menu....382
13.5 Network Menu....383
13.5.1 Modify parameter....384
13.6 Startup Select....385
13.6.1 Display Startup....386
13.6.2 Set Boot File....387
13.6.3 Set Config File....388

 Copyright © Huawei Technologies Co., Ltd.

13.6.4 Startupfile Check Manage 389
13.7 File Manager 391
13.8 Password Manager 393
13.9 FAQ About the BootROM Menu 394
13.9.1 How Do I Log in to the Device Using BootROM If I Forget the Console Login Password 394
14 BootLoader Menu on the AR3600 397
14.1 Overview of the BootLoader Menu 397
14.2 Licensing Requirements and Limitations for the BootLoader Menu 398
14.3 BootLoader Menu 398
14.4 Serial SubMenu 400
14.5 Ethernet SubMenu 401
14.5.1 Modify Parameters 402
14.6 Modify Startup Parameters 403
14.6.1 Display Current Startup Configuration 404
14.6.2 Modify Startup Boot File 404
14.6.3 Modify Startup Configuration File 405
14.6.4 Startupfile Check Manage 406
14.7 File System 407
14.8 Password Manager 409
14.9 Configuration Examples for the BootLoader Menu on the AR3600 410
14.9.1 How to Log In to the Device Through the BootLoader If I Forget the Console Port Password 410
15 Android OS Management 413
15.1 Licensing Requirements and Limitations for Android OS Management 413
15.2 Logging In to and Operating the Android OS 414
15.3 Deploying APPs 416
15.4 System Upgrade 420
15.4.1 Upgrading the System Using a USB Flash Drive 420
15.4.2 Upgrading the System Through the Upgrade Server 421
15.5 USB-based Deployment in the Android OS 424
15.5.1 USB-based Deployment Using Only the Android OS Software 425
15.5.2 USB-based Deployment Using Only the Configuration File 427
15.5.3 USB-based Deployment Using the Android OS Software and Configuration File 428
15.5.4 Setting the Password of the Compressed Configuration File for USB-based Deployment 431
15.6 FAQ About Android OS Management 432
15.6.1 How Do I Configure the Screen Rotation Function? 432
15.6.2 How Do I Set the Screen Resolution? 433
15.6.3 How Do I Configure Display Settings? 434
16 Smart Upgrade Configuration 436
16.1 Overview of Smart Upgrade 436
16.2 Smart Upgrade Process 437
16.3 Licensing Requirements and Limitations for Smart Upgrade 439

 Copyright © Huawei Technologies Co., Ltd.

16.4 Configuring Smart Upgrade..... 439
16.5 Example for Configuring Smart Upgrade..... 441

1 Overview of CLIs

About This Chapter

This chapter describes how to perform configuration and routine maintenance on devices by running commands.

1.1 Licensing Requirements and Limitations for CLIs
This section provides the Licensing Requirements and Limitations for CLIs.

1.2 How to Use Command Lines
This section describes how to use command lines and some techniques to improve operating efficiency.

1.3 Displaying the Command Output
This section describes how to query the configuration information about command lines, control the method in which command outputs are displayed, and filter the command outputs.

1.4 FAQ of CLIs

1.1 Licensing Requirements and Limitations for CLIs

This section provides the Licensing Requirements and Limitations for CLIs.

Involved Network Elements

None

Licensing Requirements

CLI overview function is a basic feature of a router and is not under license control.

Feature Limitations

None

 Copyright © Huawei Technologies Co., Ltd.

1.2 How to Use Command Lines

This section describes how to use command lines and some techniques to improve operating efficiency.

1.2.1 Entering Command Views

The device has many functions; therefore various configuration commands and query commands are provided to facilitate device management and maintenance. Huawei router registers commands to different command views based on the functions of the commands so that users can easily use them. To configure a function, enter the corresponding command view and then run corresponding commands.

The device provides various command views. For the methods of entering the command views except the following views, see the *Huawei AR Series Access Routers Command Reference*.

Common Command Views

Name	How To Enter	Function
User view	When a user logs in to the device, the user enters the user view and the following prompt is displayed: <Huawei>	In the user view, you can view the running status and statistics of the device.
System view	Run the **system-view** command and press **Enter** in the user view. The system view is displayed. <Huawei> **system-view** Enter system view, return user view with Ctrl+Z. [Huawei]	In the system view, you can set the system parameters of the device, and enter other function views from this view.

 Copyright © Huawei Technologies Co., Ltd.

Name	How To Enter	Function
Interface view	Run the **interface** command and specify an interface type and number to enter the interface view. [Huawei] **interface gigabitethernet** *X/Y/Z* [Huawei-GigabitEthernet*X/Y/Z*] *X/Y/Z* indicates the number of an interface that needs to be specified. It is in the format of slot number/card number/interface sequence number. The interface GigabitEthernet is used as an example.	In the interface view, you can configure interface parameters including physical attributes, link layer protocols, and IP addresses.
Routing protocol view	Run a command to activate a routing protocol process in the system view. The corresponding routing protocol view is displayed. [Huawei] **isis** [Huawei-isis-1]	In routing protocol views, you can configure most routing protocol parameters. The routing protocol views include the IS-IS view, OSPF view, and RIP view.

The command line prompt Huawei is the default host name (sysname). The prompt indicates the current view. For example, <> indicates the user view and [] indicates all other views except the user view.

NOTE

- Some commands can be executed in multiple views, but they have different functions after being executed in different views. For example, you can run the **lldp enable** command in the system view to enable LLDP globally and in the interface view to enable LLDP on an interface.
- In the system view, you can run the **diagnose** command to enter the diagnostic view. Diagnostic commands are used for device fault diagnosis. If you run some commands in the diagnostic view, the device may fail to run properly or services may be interrupted. Contact technical support personnel and use these diagnostic commands with caution.

Exiting Command Views

You can run the **quit** command to return from the current view to an upper-level view.

For example, after you run the **quit** command to return from the AAA view to the system view, you can run the **quit** command again to return from the system view to the user view.

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-aaa] quit
[Huawei] quit
<Huawei>
```

To return from the AAA view directly to the user view, press **Ctrl+Z** or run the **return** command.

Press **Ctrl+Z** to return directly to the user view.

```
[Huawei-aaa]          // Enter Ctrl+Z
<Huawei>
```

Run the **return** command to return directly to the user view.

```
[Huawei-aaa] return
<Huawei>
```

1.2.2 Setting Command Levels

The system divides commands into four levels and sets the command level in the specified view. The device administrator can change the command level as required, so that a lower-level user can use some high-level commands. The device administrator can also change the command level to a larger value to improve device security.

Context

- The system grants users different access permissions based on their roles. User levels are classified into sixteen levels, which correspond to the command levels. Users can use only the commands at the same or lower level than their own levels. By default, there are four command levels 0 to 3 and sixteen user levels 0 to 15. **Table 1-1** describes the relationship between command levels and user levels.

Table 1-1 Relationship between command levels and user levels

User Level	Command Level	Name	Description
0	0	Visit level	Commands of this level include network diagnosis tool commands (such as ping and tracert), commands for accessing external devices from the local device (such as Telnet) and some display commands.
1	0, 1	Monitoring level	Commands of this level are used for system maintenance, including display commands. **NOTE** Some display commands are not at this level. For example, the **display current-configuration** and **display saved-configuration** commands are at level 3. For details about command levels, see the *Huawei AR Series Access Routers Command Reference*.

 Copyright © Huawei Technologies Co., Ltd.

User Level	Command Level	Name	Description
2	0, 1, 2	Configuration level	Commands of this level are used for service configuration to provide direct network services, including routing commands and commands of each network layer.
3 to 15	0, 1, 2, 3	Management level	Commands of this level are used for basic system operations, including file system, FTP, TFTP download, user management, command level configuration, and debugging.

NOTICE

Changing the default command level without the guidance of technical personnel is not recommended. This may result in inconvenience for operation and maintenance and bring about security problems.

Procedure

Step 1 Run **system-view**

The system view is displayed.

Step 2 (Optional) Run **display command-view** *command-key*

The view of a specified command is displayed.

You can perform this step to check the view of the command whose level needs to be changed.

Step 3 Run **command-privilege level** *level* **view** *view-name command-key*

The command level is set in the specified view.

----End

1.2.3 Editing Command Lines

Editing Feature

You can edit commands in a CLI that supports multi-line edition. Each command can contain a maximum of 510 characters. The keywords in the commands are case insensitive. Whether a command parameter is case sensitive or not depends on what the parameter is.

Table 1-2 lists keys that are frequently used for command editing.

 Copyright © Huawei Technologies Co., Ltd.

Table 1-2 Keys for command editing

Key	Function
Common key	Inserts a character at the current location of the cursor if the editing buffer is not full, and the cursor moves to the right. Otherwise, an alarm is generated.
Backspace	Deletes the character on the left of the cursor and the cursor moves to the left. When the cursor reaches the head of the command, an alarm is generated.
Left cursor key ← or Ctrl+B	Moves the cursor to the left by the space of a character. When the cursor reaches the head of the command, an alarm is generated.
Right cursor key → or Ctrl+F	Moves the cursor to the right by the space of a character. When the cursor reaches the end of the command, an alarm is generated.

Operating Techniques

Incomplete Keyword

You can enter incomplete keywords on the device. In the current view, you do not need to enter complete keywords if the entered characters can match a unique keyword. This function improves operating efficiency.

For example, to execute the **display current-configuration** command, you can enter **d cu**, **di cu**, or **dis cu**, but you cannot enter **d c** or **dis c** because they do not match unique keywords.

NOTICE

The maximum length of a command (including the incomplete command) to be entered is 510 characters. If a command in incomplete form is configured, the system saves the command to the configuration file in its complete form, which may cause the command to have more than 510 characters. In this case, the command in incomplete form cannot be restored after the system restarts. Therefore, when you configure a command in incomplete form, pay attention to the length of the command.

Tab

Enter an incomplete keyword and press Tab to complete the keyword.

- When a unique keyword matches the input, the system replaces the incomplete input with the unique keyword and displays it in a new line with the cursor leaving a space behind. For example:
  a. Enter an incomplete keyword.
     ```
     [Huawei] info-
     ```
  b. Press **Tab**.

 Copyright © Huawei Technologies Co., Ltd.

The system replaces the entered keyword and displays it in a new line with the complete keyword followed by a space.

```
[Huawei] info-center
```

- When the input has multiple matches, press Tab repeatedly to display the keywords beginning with the incomplete input in a circle until the desired keyword is displayed. In this case, the cursor closely follows the end of the keyword. For example:

  a. Enter an incomplete keyword.

  ```
  [Huawei] info-center log
  ```

  b. Press **Tab**.

  The system displays the prefixes of all the matched keywords. In this example, the prefix is **log**.

  ```
  [Huawei] info-center logbuffer
  ```

  Press **Tab** to switch from one matched keyword to another. In this case, the cursor closely follows the end of a word.

  ```
  [Huawei] info-center logfile
  [Huawei] info-center loghost
  ```

  Stop pressing **Tab** when the desired keyword is displayed.

- When an incorrect keyword is entered, press Tab and it is displayed in a new line without being changed. For example:

  a. Enter an incorrect keyword.

  ```
  [Huawei] info-center loglog
  ```

  b. Press **Tab**.

  ```
  [Huawei] info-center loglog
  ```

  The system displays information in a new line, but the keyword **loglog** remains unchanged and there is no space between the cursor and the keyword, indicating that this keyword does not exist.

1.2.4 Using Command Line Online Help

When using a command line, you can use the online help to obtain real-time help without memorizing a large number of complex commands.

When entering command lines, you can enter a question mark (?) at any time to obtain online help. You can choose to obtain full help or partial help.

Full Help

When entering a command, you can use the full help function to obtain keywords and parameters for the command. Use any of the following methods to obtain full help from a command line.

- Enter a question mark (?) in any command view to obtain all the commands and their simple descriptions. For example:

```
<Huawei> ?
User view commands:
  arp-ping       ARP-ping
  autosave       <Group> autosave command group
  backup         Backup  information
  cd             Change current directory
  clear          Clear
  clock          Specify the system clock
  cls            Clear screen
  compare        Compare configuration file
```

 Copyright © Huawei Technologies Co., Ltd.

```
  copy          Copy from one file to another
...
```

- Enter some keywords of a command and a question mark (?) separated by a space. All keywords associated with this command, as well as simple descriptions, are displayed. For example:

```
<Huawei> system-view
[Huawei] user-interface vty 0 4
[Huawei-ui-vty0-4] authentication-mode ?
  aaa       AAA authentication
  password  Authentication through the password of a user terminal interface
[Huawei-ui-vty0-4] authentication-mode aaa ?
  <cr>  Please press ENTER to execute command
[Huawei-ui-vty0-4] authentication-mode aaa
```

  - "aaa" and "password" are keywords. "AAA authentication" and "Authentication through the password of a user terminal interface" describe the keywords respectively.
  - <cr> indicates that there is no keyword or parameter in this position. You can press Enter to run this command.

- Enter some keywords of a command and a question mark (?) separated by a space. All parameters associated with this keyword, as well as simple descriptions, are listed. For example:

```
<Huawei> system-view
[Huawei] ftp timeout ?
  INTEGER<1-35791>  The value of FTP timeout (in minutes)
[Huawei] ftp timeout 35 ?
  <cr>  Please press ENTER to execute command
[Huawei] ftp timeout 35
```

  "INTEGER<1-35791>" describes the value range of the parameter. "The value of FTP timeout (in minutes)" briefly describes the function of this parameter.

Partial Help

If you enter only the first or first several characters of a command keyword, partial help provides keywords that begin with this character or character string. Use any of the following methods to obtain partial help from a command line.

- Enter a character string followed directly by a question mark (?) to display all keywords that begin with this character string. For example:

```
<Huawei> d?
  debugging  <Group> debugging command group
  delete     Delete a file
  dialer     Dialer
  dir        List files on a filesystem
  display    Display information
<Huawei> d
```

- Enter a command and a string followed directly by a question mark (?) to display all the keywords that begin with this string. For example:

```
<Huawei> display b?
  bfd              Specify BFD(Bidirectional Forwarding Detection)
                   configuration information
  bgp              BGP information
  binding          Display binding relation of profile
  bridge           <Group> bridge command group
```

- Enter the first several letters of a keyword in a command and press **Tab** to display a complete keyword. The first several letters, however, must uniquely identify the keyword. If they do not identify a specific keyword, press **Tab** continuously to display different keywords and you can select one as required.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The command output obtained through the online help function is used for reference only.

1.2.5 Interpreting Command Line Error Messages

If a command is entered and passes syntax check, the system executes it. Otherwise, the system reports an error message.

Table 1-3 lists the common error messages.

Table 1-3 Common error messages of the command line

Error Message	Cause of the Error
Error: Unrecognized command found at '^' position.	No command is found.
	No keyword is found.
Error: Wrong parameter found at '^' position.	The parameter type is incorrect.
	The parameter value exceeds the limit.
Error: Incomplete command found at '^' position.	The entered command is incomplete.
Error: Too many parameters found at '^' position.	Too many parameters are entered.
Error: Ambiguous command found at '^' position.	Indefinite command is entered.

1.2.6 Using the undo Command Line

If a command line begins with the keyword **undo**, it is an **undo** command line. The **undo** command lines restore default settings of parameters, disable functions, or delete configurations. Almost each configuration command line has a corresponding **undo** command.

Some examples of using the undo command are listed as follows:

- The **undo** command restores the default setting.

  The **sysname** command sets a device host name. For example:

  ```
  <Huawei> system-view
  [Huawei] sysname Server
  [Server] undo sysname
  [Huawei]
  ```

- The **undo** command disables a specified function.

  The **ftp server enable** command enables the FTP server function on the device. For example:

  ```
  <Huawei> system-view
  [Huawei] ftp server enable
  Info: Succeeded in starting the FTP server
  [Huawei] undo ftp server
  Info: Succeeded in closing the FTP server.
  ```

 Copyright © Huawei Technologies Co., Ltd.

- The **undo** command deletes a specified configuration.

  The **header** command configures the header information displayed on terminals when users log in. For example:

  ```
  <Huawei> system-view
  [Huawei] header login information "Hello,Welcome to Huawei!"
  ```

  Log out of the terminal and re-log in. A message "Hello, Welcome to Huawei!" is displayed before authentication. Run the **undo header login** command.

  ```
  Hello,Welcome to Huawei!

  Login authentication


  Password:
  <Huawei> system-view
  [Huawei] undo header login
  ```

  Log out of the terminal and re-log in. No message is displayed before authentication.

  ```
  Login authentication


  Password:
  <Huawei>
  ```

  NOTE

  The command output provided here is used for reference only. The actual output information may differ from the preceding information.

1.2.7 Displaying History Commands

The device automatically stores history commands entered by a user. To enter a command that has been executed, you can use this function to call up the history command.

By default, the system saves 10 history commands for each user. Run the **history-command max-size** *size-value* command to reset the number of history commands that can be saved in a specified user interface view. The maximum number is 256.

NOTE

If the value specified in the **history-command max-size** *size-value* command is large, it may take a long time to obtain a required history command. Therefore, a large value is not recommended.

Table 1-4 shows operations on history commands.

Table 1-4 Accessing history commands

Action	Command or Key	Result
Display history commands.	**display history-command**	The history commands entered by the current user are displayed.

 Copyright © Huawei Technologies Co., Ltd.

Action	Command or Key	Result
Display the earlier history command.	Up arrow key ↑ or Ctrl+P	An earlier history command is displayed. If the current command is the first command, an alarm is generated when you attempt to display the earlier history command.
Display the later history command.	Down arrow key ↓ or Ctrl+N	A later history command is displayed. If the current command is the latest command, no output is displayed and an alarm is generated when you attempt to display the later history command.

When using history commands, note the following:

- The saved history commands are the same as those entered by users. For example, if the user enters an incomplete command, the saved command also is incomplete.
- If the user runs the same command several times, only the latest command is saved. If the command is entered in different forms, they are considered as different commands.

  For example, if the **display current-configuration** command is run several times, only one history command is saved. If the **display current-configuration** command and the **dis curr** command are used, both of them are saved.

1.2.8 Using Command Line Shortcut Keys

You can use shortcut keys provided by the device to quickly enter commands.

There are two types of shortcut keys:

- User-defined shortcut keys: include Ctrl+G, Ctrl+L, Ctrl+O, and Ctrl+U. You can associate these shortcut keys with any commands. When a shortcut key is pressed, the system runs the corresponding command.
- System-defined shortcut keys: shortcut keys defined in the system that have fixed functions. Users cannot define these shortcut keys. **Table 1-5** lists the frequently used system-defined shortcut keys.

NOTE

The terminal in use may affect the functions of the shortcut keys. For example, if the shortcut keys defined by the terminal conflict with those defined in the system, the shortcut keys entered by the user are captured by the terminal program and the commands corresponding to the shortcut keys are not executed.

 Copyright © Huawei Technologies Co., Ltd.

User-defined Shortcut Keys

When a user frequently uses a command or some commands, the user can use shortcut keys to define these commands. Only management-level users have the rights to define shortcut keys. The configurations are as follows:

1. Run the **system-view** command to enter the system view.
2. Run the **hotkey** { **CTRL_G** | **CTRL_L** | **CTRL_O** | **CTRL_U** } *command-text* command to configure a shortcut key corresponding to a command.

The system supports four user-defined shortcut keys and the default values are as follows:

- Ctrl+G: **display current-configuration**
- Ctrl+L: **undo idle-timeout**
- Ctrl+O: **undo debugging all**
- Ctrl+U: Null

NOTE

- When defining shortcut keys, use double quotation marks to define the command if this command contains several keywords separated by spaces. For example, **hotkey ctrl_l "display tcp status"**. Do not use double quotation marks to define a command if the command contains only one keyword.
- Run the **display hotkey** command to view the status of the defined, undefined, and system-defined shortcut keys.
- Run the **undo hotkey** command to restore default values of the configured shortcut keys.
- Shortcut keys are executed in the same way as commands. The system can record commands in their original formats in the command buffer and logs to help query and locate the fault.
- The user-defined shortcut keys are available to all users. If a user does not have the rights to use the command defined by a shortcut key, the system displays an error message when this shortcut key is executed.

System-defined Shortcut Keys

Table 1-5 System-defined shortcut keys

Key	Function
Ctrl+A	Moves the cursor to the beginning of the current line.
Ctrl+B	Moves the cursor back one character.
Ctrl+C	Stops performing current functions.
Ctrl+D	Deletes the character where the cursor is located at.
Ctrl+E	Moves the cursor to the end of the last line.
Ctrl+F	Moves the cursor forward one character.

 Copyright © Huawei Technologies Co., Ltd.

Key	Function
Ctrl+H	Deletes the character on the left side of the cursor.
Ctrl+K	Stops outgoing connections in the call establishment stage.
Ctrl+N	Displays the next command in the history command buffer.
Ctrl+P	Displays the previous command in the history command buffer.
Ctrl+T	Function as a question mark.
Ctrl+W	Deletes a character string on the left side of the cursor.
Ctrl+X	Deletes all the characters on the left side of the cursor.
Ctrl+Y	Deletes all the characters on the right side of the cursor and the character where the cursor is located at.
Ctrl+Z	Returns to the user view.
Ctrl+]	Stops incoming connections or redirects the connections.
Esc+B	Moves the cursor back one word.
Esc+D	Deletes one word on the right side of the cursor.
Esc+F	Moves the cursor forward one word.

1.2.9 Executing Commands in a Batch

If multiple commands are frequently used consecutively, you can edit these commands to be executed in batches. This simplifies command input and improves efficiency.

Procedure

- Configure assistant tasks to automatically run commands in a batch at scheduled time.

  You can configure one or more scheduled tasks to realize automatic O&M. The device can then run one or a group of commands at specified time or after a certain delay. Assistant tasks enable the device to complete specified operations or configuration without human intervention. Assistant tasks are usually used for scheduled upgrading or configuration.

 Copyright © Huawei Technologies Co., Ltd.

a. Run the **system-view** command to enter system view.

b. Run the **assistant task** *task-name* command to create an assistant task. You can create a maximum of five assistant tasks.

c. Run the **if-match timer cron** *seconds minutes hours days-of-month months days-of-week* [*years*] command to specify the time when the assistant tasks work.

d. Run the **perform** *priority* **batch-file** *filename* command to configure the operations of assistant tasks.

NOTE

By default, the commands listed in the batch file are executed in the system view.

e. Run the **display assistant task history** [*task-name*] command to view the operation records of task assistants.

This function promotes the automatic control and management abilities of the device, reducing power consumption.

----End

1.3 Displaying the Command Output

This section describes how to query the configuration information about command lines, control the method in which command outputs are displayed, and filter the command outputs.

1.3.1 Verifying Command Line Configurations

After the configurations are complete, you can run the **display** command to verify the configuration and running information on the device.

For example, after all configurations of the FTP service are complete, you can run the **display ftp-server** command to check parameters of the FTP server. For details on the usage and functions of the **display** command, see Checking the Configuration in each feature of the *Configuration Guide*.

You can also verify the current running configurations and configurations in the current view.

- Verify the current running configurations:

  display current-configuration

  This command does not display parameters that use default settings.

- Verify configurations in the current view:

  display this

  This command does not display parameters that use default settings.

  NOTE

  When a user runs the **display this** command to check configuration information, other users can run this same command only after all the command output is displayed.

 Copyright © Huawei Technologies Co., Ltd.

1.3.2 Configuring Users of Different Levels to View Different Configurations

The device allows users of different levels to view specified configurations, so users can view outputs of specified command lines.

Context

After the administrator runs the **command-privilege level** command to degrade the level of **display current-configuration**, low-level users can run the **display current-configuration** command to view all device configurations.

To allow the low-level users to view the specified configurations, the administrator can run the **set current-configuration display** command to specify the configurations to be displayed.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **command-privilege level** *level* **view** *view-name command-key* command to specify the level of the **display current-configuration** command.

Step 3 Run the **set current-configuration display** [**all**] **level** *level command-key* command to specify the configuration that a user of a specified level can view.

----End

Verifying the Configuration

Log in to the device as a user of the specified level and run the **display current-configuration** command.

1.3.3 Controlling the Display Mode of Commands

When running commands, you can specify the display mode.

- When the display output is more than one page, you can use **Pg Up** and **Pg Dn** to display information on the previous page and the next page.
- When the information cannot be completely displayed on one screen, the system will pause and you can view the information. You can use the function keys listed in **Table 1-6** to control the display mode of command lines.

  NOTE

  The **screen-length** *screen-length* **temporary** command sets the lines to be displayed temporarily on the terminal screen. If *screen-length* is 0, the split screen function is disabled. Therefore, the system will not pause when the information cannot be completely displayed on one screen.

 Copyright © Huawei Technologies Co., Ltd.

Table 1-6 Display mode of commands

Key	Function
Ctrl+C or Ctrl+Z	Stops displaying information and running commands. **NOTE** You can also press any key (the number key or letter key) except space and Enter.
Space	Continues to display the next screen of information.
Enter	Continues to display the next line of information.

1.3.4 Filtering Command Outputs

When running the **display** command to check the command output, you can use the regular expression (specifying the rule to display) to filter the output information and locate needed information quickly.

Regular Expressions

A regular expression is a mode matching tool. It consists of common characters (such as letters) and special characters (called meta-characters). The regular expression is a template according to which you can search for the required string.

A regular expression provides the following functions:

- Searches for and obtains a sub-string that matches a rule in the string.
- Substitutes a string based on a certain matching rule.

The regular expression consists of common characters and special characters.

- Common characters

  Common characters are used to match themselves in a string, including all upper-case and lower-case letters, digits, punctuations, and special symbols. For example, a matches the letter "a" in "abc", 10 matches the digit "10" in "10.113.25.155", and @ matches the symbol "@" in "xxx@xxx.com".
- Special characters

  Special characters are used together with common characters to match the complex or special string combination. **Table 1-7** describes special characters and their syntax.

 Copyright © Huawei Technologies Co., Ltd.

Table 1-7 Description of special characters

Special Characters	Function	Example
\	Defines an escape character, which is used to mark the next character (common or special) as the common character.	* matches "*".
^	Matches the starting position of the string.	^10 matches "10.10.10.1" instead of "20.10.10.1".
$	Matches the ending position of the string.	1$ matches "10.10.10.1" instead of "10.10.10.2".
*	Matches the preceding element zero or more times.	10* matches "1", "10", "100", "1000", and so on. (10)* matches "null", "10", "1010", "101010", and so on.
+	Matches the preceding element one or more times.	10+ matches "10", "100", "1000", and so on. (10)+ matches "10", "1010", "101010", and so on.
?	Matches the preceding element zero or one time.	10? matches "1" or "10". (10)? matches "null" or "10".
.	Matches any single character.	0.0 matches "0x0", "020", and so on. .oo. matches "book", "look", "tool", and so on.
()	Defines a subexpression, which can be null. Both the expression and the subexpression should be matched.	100(200)+ matches "100200", "100200200", and so on.
x|y	Matches x or y.	100|200 matches "100" or "200". 1(2|3)4 matches "124" or "134", instead of "1234", "14", "1224", and "1334".
[xyz]	Matches any single character in the regular expression.	[123] matches the character 2 in "255".
[^xyz]	Matches any character that is not in the regular expression.	[^123] matches any character except for "1", "2", and "3".
[a-z]	Matches any character within the specified range.	[0-9] matches any character ranging from 0 to 9.

 Copyright © Huawei Technologies Co., Ltd.

Special Characters	Function	Example
[^a-z]	Matches any character beyond the specified range.	[^0-9] matches all non-numeric characters.
_	Matches a comma ",", left brace "{", right brace "}", left parenthesis "(", and right parenthesis ")". Matches the starting position of the input string. Matches the ending position of the input string. Matches a space.	_2008_ matches "2008", "space 2008 space", "space 2008", "2008 space", ",2008,", "{2008}", "(2008)", "{2008)", and "(2008}".

NOTE

Unless otherwise specified, all the characters in the preceding table must be printable characters.

- Degeneration of special characters

  Certain special characters, when placed at certain positions in a regular expression, degenerate to common characters.

  - The special characters following "\" match special characters themselves.
  - The special characters "*", "?", and "+" are placed at the starting position of the regular expression. For example, +45 matches "+45" and abc(*def) matches "abc*def".
  - The special character "^" is placed at any position except for the start of the regular expression. For example, abc^ matches "abc^".
  - The special character "$" is placed at any position except for the end of the regular expression. For example, 12$2 matches "12$2".
  - A right parenthesis ")" or right bracket "]" is not paired with a corresponding left parenthesis "(" or bracket "[". For example, abc) matches "abc)" and 0-9] matches "0-9]".

  NOTE

  Unless otherwise specified, degeneration rules also apply when the preceding regular expressions are subexpressions within parentheses.

- Combination of common and special characters

  In actual usage, regular expressions combine multiple common and special characters to match certain strings.

 Copyright © Huawei Technologies Co., Ltd.

Specifying a Filtering Mode in a Command

NOTE

- The device uses a regular expression to implement the pipe character filtering function. A display command supports the pipe character only when there is excessive output information.
- When filtering conditions are set to query output information, the first line of the command output starts with the entire regular expression but not the string to be filtered.

The system allows you to use **| count** to display the number of lines and **| section** to display the command output by section after using filtering mode. **| count** and **| section** can work together with the following filtering modes.

Three filtering modes are provided for commands that support regular expressions.

- **| begin** *regular-expression*: displays all the lines beginning with the line that matches the regular expression.

  Filter the character strings to be entered until the specified case-sensitive character string is displayed. All the character strings following this specified character string are displayed on the screen.
- **| exclude** *regular-expression*: displays all the lines that do not match the regular expression.

  If the character strings to be entered do not contain the specified case-sensitive character string, they are displayed on the screen. Otherwise, they are filtered.
- **| include** *regular-expression*: displays all the lines that match the regular expression.

  If the character strings to be entered contain the specified case-sensitive character string, they are displayed on the screen. Otherwise, they are filtered.

NOTE

The value of *regular-expression* is a string of 1 to 255 characters. *regular-expression* cannot contain underlines ([).

The following examples describe how to specify a filter mode in a command.

Example 1: Run the **display interface brief** command to display all the lines that do not match the regular expression Ethernet|NULL|Tunnel. Ethernet|NULL|Tunnel matches Ethernet, NULL or Tunnel.

```
<Huawei> display interface brief | exclude Ethernet|NULL|Tunnel
PHY: Physical
*down: administratively down
(l): loopback
(s): spoofing
(b): BFD down
^down: standby
(e): ETHOAM down
(d): Dampening Suppressed
InUti/OutUti: input utility/output utility
Interface                   PHY   Protocol InUti OutUti   inErrors  outErrors
LoopBack1                     up    up(s)     0%     0%          0          0
Vlanif7                     up    up         --     --          0          0
Vlanif10                    up    up         --     --          0          0
Vlanif19                    up    up         --     --          0          0
```

 Copyright © Huawei Technologies Co., Ltd.

```
Vlanif60                up    up         --    --         0         0
Vlanif66                down  down       --    --         0         0
Vlanif70                down  down       --    --         0         0
Vlanif77                up    up         --    --         0         0
Vlanif100               down  down       --    --         0         0
```

Example 2: Run the **display current-configuration** command to display all the lines that match the regular expression vlan.

```
<Huawei> display current-configuration | include vlan
vlan batch 7 10 18 to 19 30 60 66 70 77 100 105
vlan batch 200 1024
 port default vlan 77
 port default vlan 19
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 port hybrid pvid vlan 60
 undo port hybrid vlan 1
 port hybrid tagged vlan 60
 port trunk allow-pass vlan 60
 port hybrid pvid vlan 10
 port hybrid tagged vlan 7
 port hybrid untagged vlan 10
```

NOTE

The preceding information is used for reference only.

1.4 FAQ of CLIs

1.4.1 What Are Shortcut Keys ESC_B and ESC_F For?

ESC_B moves the cursor forward one word, whereas ESC_F moves the cursor back one word.

1.4.2 How Do I Define the Command Level?

The administrator can run the **command-privilege level** *level* **view** *view-name command-key* command to set the command level in a specified view. This configuration enables a lower-level user to use some high-level commands, or raises the command level to improve device security.

NOTICE

It is recommended that you do not change the default command level without the guidance of professionals. Otherwise, it may result in inconvenience for operation and maintenance and bring about security problems.

```
<Huawei> system-view
[Huawei] command-privilege level 5 view user save
```

 Copyright © Huawei Technologies Co., Ltd.

2 Auto-Config Configuration

About This Chapter

Auto-Config enables a device to automatically load version files including system software, patch files and configuration files. This simplifies configuration. Devices can be managed in a centralized manner and debugged remotely.

2.1 Overview of Auto-Config
This section describes definition of Auto-Config and purpose of this feature.

2.2 Understanding Auto-Config
This section describes implementation of Auto-Config.

2.3 Application Scenarios for Auto-Config
This section describes application scenarios for the Auto-Config feature.

2.4 Licensing Requirements and Limitations for Auto-Config
This section provides prerequisites for configuring Auto-Config, interfaces that support Auto-Config, and configuration notes.

2.5 Default Settings for Auto-Config
This section provides the default settings for Auto-Config.

2.6 Configuring Auto-Config on Devices that are on the Same Network Segment with the DHCP Server
The device to be configured that is on the same network segment as the DHCP server can be configured with Auto-Config to automatically load the system software, patch file, and configuration file, realizing remote device deployment.

2.7 Configuring Auto-Config Across Different Network Segments
The device that is on a different network segment than the DHCP server can have Auto-Config configured to automatically load the system software, patch file, and configuration file for remote device deployment.

2.8 Maintaining Auto-Config
You can monitor the running status of Auto-Config in each phase to ensure that Auto-Config runs normally.

2.9 Configuration Examples for Auto-Config

 Copyright © Huawei Technologies Co., Ltd.

This section provides Auto-Config configuration examples including networking requirements and configuration roadmap.

2.1 Overview of Auto-Config

This section describes definition of Auto-Config and purpose of this feature.

Definition

Auto-Config enables devices to be configured must be new devices or have no configuration files to automatically load version files including system software, patch files, configuration files when the device starts up.

Purpose

After devices are deployed on the network, software engineers need to commission the software onsite. If a large number of devices are sparsely distributed on the network, maintenance personnel need to manually configure each device, which lowers device deployment efficiency and increases costs. Auto-Config enables devices to automatically obtain version files from the file server and automatically load them, realizing remote deployment of network devices. This reduces costs and increases device deployment efficiency.

2.2 Understanding Auto-Config

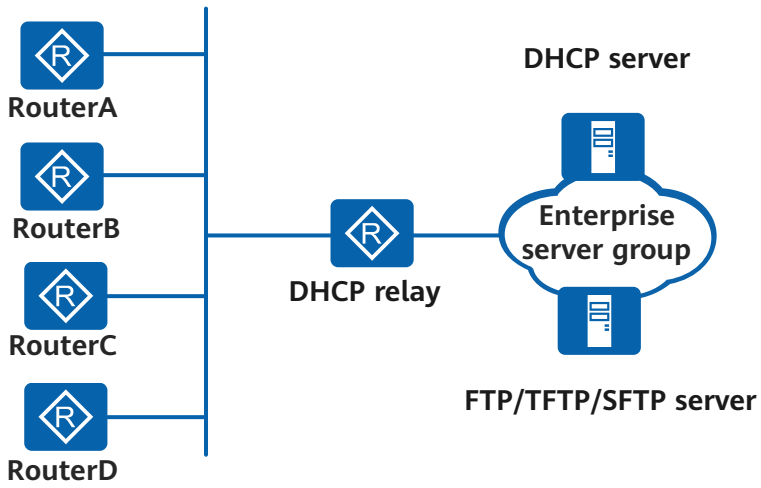
This section describes implementation of Auto-Config.

2.2.1 Auto-Config Fundamentals

In **Figure 2-1**, Auto-Config runs on Router A, Router B, Router C, and Router D. These devices function as DHCP clients and periodically send DHCP Request packets to the **DHCP server** to obtain configuration. The DHCP server responds with DHCP Reply packets that contain information about IP addresses assigned to devices to be configured, the IP address of the **file server**, the file server login method, and configuration of version files (the configuration of version files can be obtained through the **intermediate file**. The intermediate file must be configured in advance and saved on the file server). After receiving the DHCP Reply packets, devices obtain version files from the file server and automatically load version files after restarting.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-1 Auto-Config networking diagram



Concepts

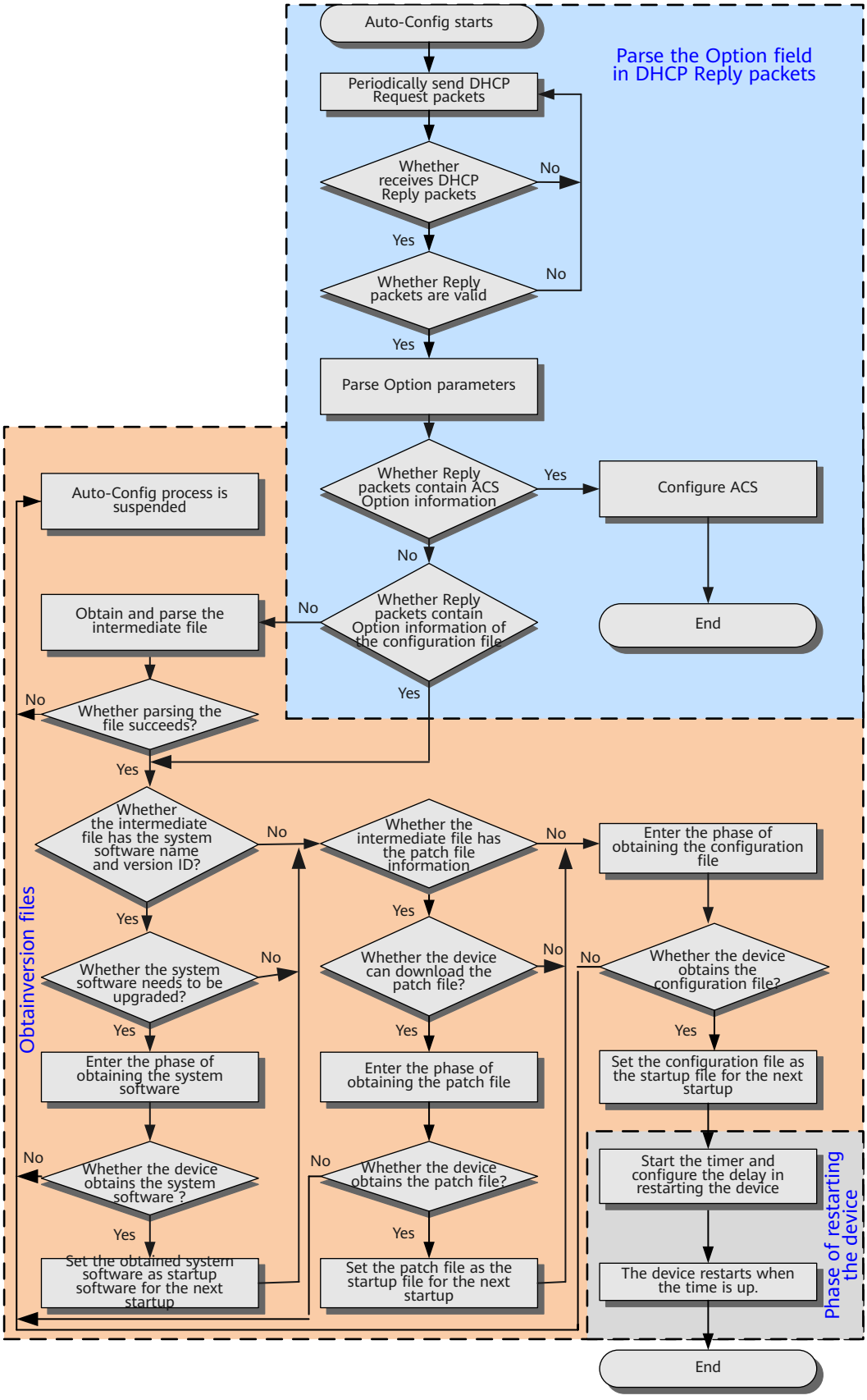
- **DHCP server**: When Auto-Config starts running on devices, these devices function as DHCP clients to send DHCP Request packets to the DHCP server for network configuration. The dynamic IP address pool, egress gateway address, and **2.2.3 Option Parameters** need to be configured on the DHCP server. The dynamic IP address pool assigns IP addresses to interfaces on devices. Option parameters contain information about the IP address of the file server, and the name of the version file to be loaded.
- **DHCP relay**: If the device to be configured is on a different network segment than the DHCP server, DHCP relay needs to be configured to allow packet exchange between the device and the DHCP server.
- **File server**: It is an FTP, TFTP, or SFTP server. Version files are saved on the file server. Version files include configuration files, system software, and patch files to be loaded through Auto-Config. After receiving the IP address of the file server sent from the DHCP server, devices to be configured obtain version files from the file server and set the files as the version files for the next startup.
- **Intermediate file**: If Option 67 that contains information about the configuration file is not configured on the DHCP server, Auto-Config enables devices to obtain information about version files that need to be downloaded by parsing the intermediate file. **2.2.4 Intermediate File** is saved on the file server and contains information about mappings from system MAC address or ESN to the system software name, system software version, patch file name, and configuration file name.

2.2.2 Working Process of Auto-Config

Figure 2-2 shows the Auto-Config working process.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-2 Basic process of Auto-Config



 Copyright © Huawei Technologies Co., Ltd.

The Auto-Config process involves three phases:

- Parse the Option field in the DHCP Reply packet.
  a. Obtain information about the IP address and configuration of the file server.
     i. The device automatically enables the DHCP client function on uplink Ethernet interfaces in Up state and broadcasts DHCP Request packets (the IP address pool, Option parameters, and gateway have been configured on the DHCP server).
     ii. The DHCP server sends DHCP Reply packets to the device. These packets contain information about IP addresses of the device to be configured and the FTP/TFTP/SFTP server, FTP/SFTP user name, password, and default gateway.

     NOTE

     If no DHCP Reply packet is received or the received DHCP Reply packet is invalid, a DHCP Request packet is sent every 5 minutes. After 24 hours, a DHCP Request packet is sent every one hour.

  b. Parse Option parameters.
     i. If the received DHCP Reply packet contains Option 43, Auto-Configuration server (ACS) needs to be configured. After ACS configuration is complete, the device is configured using the Auto-Configuration server.

     NOTE

     If the DHCP server assigns ACS configuration to devices that needs to be configured, remote deployment of devices is realized through the Auto-Configuration server (for details about Auto-Config implementation through ACS, see CWMP) not the Auto-Config process. For details about CWMP, see "CWMP" in Feature Description-Network Management.

     ii. If the received DHCP Reply packet does not contain Option 67, the intermediate file is required. Then the device downloads the intermediate file from the FTP/TFTP/SFTP server and obtains information about version files that need to be downloaded from the intermediate file. The process of obtaining files is started. If the received DHCP Reply packet contains Option 67, the process of obtaining version files is started directly.
- Obtain version files.
  a. (Optional) Download the system software.
     i. Obtain the system software name and version ID from the intermediate file or the DHCP server.
     ii. Download system software from the file server and set the downloaded file as the startup file for the next startup.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- This Auto-Config process runs when the following conditions are met: System software needs to be upgraded; information about system software is configured on the DHCP server or the intermediate file; system software is saved on the file server.
- You can configure Option 146 on the DHCP server to determine whether to delete system software when the space is insufficient. The device deletes system software when the space is insufficient based on the setting of Option 146.

b. (Optional) Download the patch file.

i. Obtain information about the patch file from the intermediate file or the DHCP Reply packets.

ii. Download the patch file from the file server and set the downloaded file as the startup file for the next startup.

NOTE

This Auto-Config process runs when the following conditions are met: The patch file needs to be upgraded; information about the patch file is configured on the DHCP server or the intermediate file; the patch file is saved on the file server.

c. Download the configuration file.

i. Obtain information about the configuration file from the intermediate file or the DHCP Reply packets.

ii. Download the configuration file from the file server and set the downloaded file as the startup file for the next startup.

NOTE

- If the system fails to obtain the intermediate file, system software, patch file, and configuration file, the system suspends the Auto-Config process and waits for human intervention. After handing the reason for the Auto-Config failure, run the **autoconfig getting-file restart** command to obtain the intermediate file, system software, patch file, and configuration file and resume the Auto-Config process.
- The Auto-Config process triggers the startup of the device through the configuration file. Therefore, the configuration file is mandatory, and the version file and patch file are optional.

- Restart the device.

  You can configure Option 146 on the DHCP server to specify the delay in restarting the device. After the configuration file is downloaded successfully, the device is restarted according to the setting of Option 146. If no Option 146 is configured, the device is restarted immediately after the configuration file is downloaded.

2.2.3 Option Parameters

A DHCP server sends DHCP packets with the Option field carrying configuration parameters to clients to implement the Auto-Config function.

Table 2-1 shows DHCP Option parameters used in Auto-Config.

 Copyright © Huawei Technologies Co., Ltd.

Table 2-1 DHCP Option parameters

Option	Description

Option 43	Configuration of the ACS server assigned to DHCP clients.
	• sub-option 1: information about ACS URL. Format:
	`URL=URL_INFO;`
	Example:
	`URL=http://192.168.1.40:80/acs;`
	• sub-option 2: ACS user name and password. Format:
	`username=USERNAME;password=PASSWORD;`
	Example:
	`username=user;password=huawei;`

Option 67	Name of the configuration file assigned to DHCP clients. **NOTE** The configuration file path can be specified, The total length of the file path and name cannot exceed 64 bytes. By default, the file path is the server's root directory. For example, if the server's root directory is flash:/, and the configuration file **vrpcfg.cfg** is saved to the config folder in the flash:/ directory, the file name with the file path can be specified as config/vrpcfg.cfg.
Option 141	FTP/SFTP user name assigned to DHCP clients.
Option 142	FTP/SFTP password assigned to DHCP clients.
Option 143	FTP server IP address assigned to DHCP clients.

Option 145	Information about the non-configuration file assigned to DHCP clients, for example: information about the system software, version ID and patch file. Format:
	`vrpfile=VRPFILENAME;vrpver=VRPVERSION;patchfile=PATCHFILENAME;`
	Example:
	`vrpfile=auto_V200R010.cc;vrpver=V200R010;patchfile=auto_V200R010.pat;`

 Copyright © Huawei Technologies Co., Ltd.

Option	Description
Option 146	User-defined settings, including file deletion policy used when memory space is insufficient and delay in activating the configuration file. Format: • opervalue = 0: indicates that no system software will be deleted from the file system when the space is insufficient. opervalue=1: indicates that system software will be deleted from the file system when the space is insufficient. By default, no file will be deleted from the file system when the space is insufficient. • delaytime: specifies the delay in restarting a device after a configuration file is downloaded to the device, in seconds. By default, the delay is 0 seconds. **NOTE** The maximum delay in restarting a device is 1 day, namely, 86400 seconds. If the configured delay exceeds 1 day, the delay is calculated as 1 day.
Option 147	Authentication information used by devices to be configured to authenticate the DHCP server for device deployment. Option 147 is optional. If Option 147 is required, it must be configured as AutoConfig.

 Copyright © Huawei Technologies Co., Ltd.

Option	Description

Option 148	Agile Controller-Branch's IP address and port number assigned to DHCP clients.
	Option 148 is in the following format:
	`agilemode=AGILEMODE;agilemanage-mode=AGILEMANAGE-MODE;agilemanage-domain=AGILEMANAGE-DOMAIN;agilemanage-port=AGILEMANAGE-PORT;`
	● agilemode: indicates the agile mode. agilemode=tradition: indicates the traditional mode.
	● agilemanage-mode: indicates that the agilemanage-domain field is an IP address or a domain name. agilemanage-mode=ip: indicates that the agilemanage-domain field is an IP address. agilemanage-mode=domain: indicates that the agilemanage-domain field is a domain name.
	● agilemanage-domain: indicates an IP address in case of agilemanage-mode=ip or indicates a domain name in case of agilemanage-mode=domain.
	● agilemanage-port: indicates the Agile Controller-Branch's port number assigned to DHCP clients.
	For example, in the Cloud VPN scenario, if the Agile Controller-Branch's IP address and port number assigned to DHCP clients are 10.17.15.84 and 10020, Option 148 is as follows:
	`agilemode=tradition;agilemanage-mode=ip;agilemanage-domain=10.17.15.84;agilemanage-port=10020;`

Option 149	SFTP server IP address and port number assigned to DHCP clients. For example, if the SFTP server IP address is 10.10.10.1 and port number is 22, the Option 149 field is: `option 149 ascii ipaddr=10.10.10.1;port=22;`
Option 150	TFTP server IP address assigned to DHCP clients.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- Option 150 enables DHCP clients to directly obtain the TFTP server IP address.
- Options 141, 142, and 143 enable DHCP clients to obtain the FTP user name, FTP password, and FTP server IP address.
- Options 141, 142, and 149 enable DHCP clients to obtain the SFTP user name, SFTP password, and SFTP server IP address and port number.
- When multiple types of Option parameters are set for a DHCP server, the priority of file servers is selected as follows: SFTP > FTP > TFTP.

2.2.4 Intermediate File

If Option 67 that contains information about the configuration file is not configured on the DHCP server, Auto-Config enables devices to obtain information about version files that need to be downloaded by parsing the intermediate file.

The intermediate file is saved on the file server and contains information about mappings from system MAC address or ESN to the system software name, system software version, patch file name, and configuration file name. After obtaining the IP address of the file server, the device downloads the intermediate file from the file server, searches for the system software name, system software version, patch file name and configuration file name that match its own MAC address or ESN, and downloads files from the file server based on the obtained file names.

For example, if the MAC address of a device is 0018-82C5-AA89, the ESN is 9300070123456789, the version file name is auto_V200R010.cc, the version is V200R010, the patch file is auto_V200R010.pat, the configuration file is auto_V200R010.cfg, the intermediate file content is as follows:

```
MAC=0018-82C5-
AA89;vrpfile=auto_V200R010.cc;vrpver=V200R010;patchfile=auto_V200R010.pat;cfgfile=auto_V200R010.cfg;
```

NOTE

- The intermediate file name is arnet.ini.
- If multiple devices are configured, each row in the intermediate file records configuration information about each device.
- When configuring the intermediate file, enter the MAC address and ESN, or either of them. The configuration file is mandatory, and the version file and patch file are optional. The three files can be configured in any sequence.
- The version file name and system software version must be available in the intermediate file, and version ID in the system software name must be the same as that in the intermediate file. The version number (vrpver) must be included in the system software information (vrpfile).

2.3 Application Scenarios for Auto-Config

This section describes application scenarios for the Auto-Config feature.

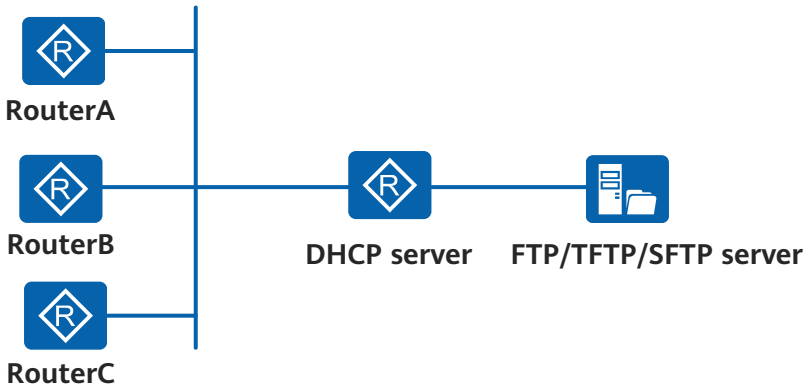
Configuring Auto-Config on Devices that are on the Same Network Segment with the DHCP Server

If a device with no configuration file is on the same network segment as the DHCP server, you can configure Auto-Config based on the networking diagram as shown in **Figure 2-3**. The configuration file (mandatory), system software

(optional), patch file (optional), and intermediate file (optional) are saved on the FTP/TFTP/SFTP server. Routes between the FTP/TFTP/SFTP server, devices to be configured (devices have obtained IP addresses), and the DHCP server are reachable. After software engineers configure the DHCP server and FTP/TFTP/SFTP server, devices can use Auto-Config to load version files including the configuration file (mandatory), system software (optional), and patch file (optional) from the FTP/TFTP/SFTP server.

This configuration method applies to a small network where devices are densely distributed.

Figure 2-3 Auto-Config networking on the same network segment



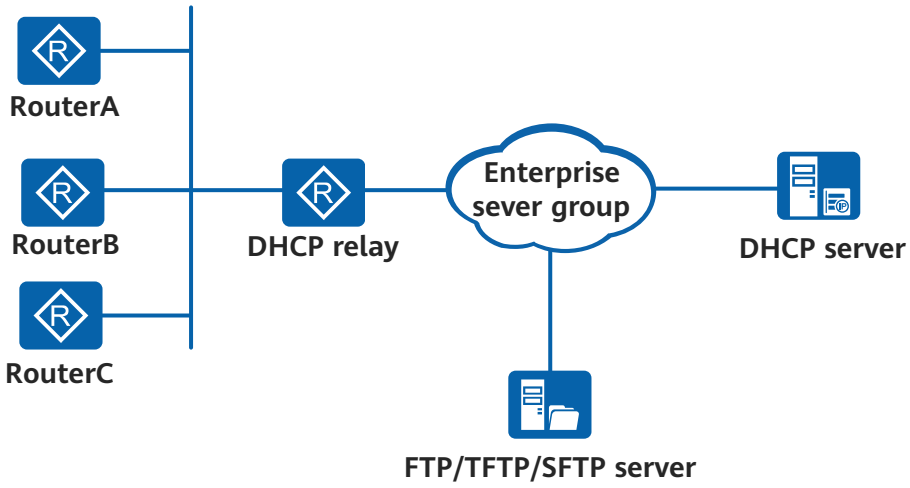
Configuring Auto-Config on Devices That are on Different Network Segments than the DHCP Server

If a device with no configuration file is on a different network segment than the DHCP server, you can configure Auto-Config based on the networking diagram as shown in **Figure 2-4**. The configuration file (mandatory), system software (optional), patch file (optional), and intermediate file (optional) are saved on the FTP/TFTP/SFTP server. Routes between the FTP/TFTP/SFTP server, devices with no configuration file (devices have obtained IP addresses), the DHCP relay agent, and DHCP server are reachable. After software engineers configure the DHCP relay agent, DHCP server and FTP/TFTP/SFTP server, devices can use Auto-Config to obtain version files including the configuration file (mandatory), system software (optional), and patch file (optional) from the FTP/TFTP/SFTP server and load version files.

This configuration method applies to a large network where devices with no configuration file are sparsely distributed. Devices on multiple network segments share one DHCP server, reducing costs and facilitating centralized management.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-4 Auto-Config networking across different network segments



2.4 Licensing Requirements and Limitations for Auto-Config

This section provides prerequisites for configuring Auto-Config, interfaces that support Auto-Config, and configuration notes.

Involved Network Elements

None

Licensing Requirements

Auto-Config is a basic feature of a router and is not under license control.

Feature Limitations

NOTE

- AR100 series, AR120 series (except AR129 and AR129GW-L), AR150 series (except AR156, AR156W, AR157, AR157G-HSPA+7, AR157VW, AR157W, AR158E, and AR158EVW), AR160 series (except AR161FW-P-M5), AR201, AR1200 series, AR2200 series, and AR3200 series support Auto-Config function.
- The management interfaces of the AR1200, AR2200, AR3200, and AR3600 series do not support the Auto-Config function.

- In deployment, you can use Auto-Config to configure the device or manually configure the device. If the device is manually configured, Auto-Config is disabled automatically.
- The device can be configured using Auto-Config or USB deployment. However, two deployment methods cannot be used together. If you need to use the Auto-Config function after USB-based deployment has been performed on the device, you need to run the **set factory-configuration from default** command to specify the default factory settings as factory settings.

 Copyright © Huawei Technologies Co., Ltd.

- When the factory settings are being restored, only unconfigured WAN interfaces support the Auto-Config function.
- Devices to be configured must be new devices, that is, no startup configuration file with file name extension **.cfg** or **.zip** exists on the device.
- You can obtain the MAC address and ESN of the device in the following ways:
  - Check the label on the device.
  - Log in to the device and run the **display system-mac** command in the diagnosis view and the **display esn** command.
- The following interfaces support the Auto-Config function:
  - AR100 series: GE0/0/4
  - AR121, AR121W, AR121GW-L: Eth0/0/4
  - AR129CGVW-L: GE0/0/4
  - AR150 series (except AR156, AR157, AR157W, AR157VW, AR157G-HSPA+7, AR158EVW and AR156W): Eth0/0/4
  - AR160 series (except AR169 and AR169G-L): GE0/0/4
  - AR160 series (AR169 and AR169G-L): GE0/0/3
  - AR200 series (except AR206, AR207, AR207V, AR207V-P, AR208E, AR207G-HSPA+7 and AR207VW): Eth0/0/8
  - AR1200 series, AR2200 series, and AR3200 series: Layer 3 Ethernet interfaces except for the management interface, GPON interface, and EPON interface

    When a GPON or EPON interface is used to implement the Auto-Config function on a device, the system automatically creates a sub-interface numbered 4094. In addition, the system sets the encapsulation mode of the sub-interface to dot1q and the VLAN tag allowed by the sub-interface to 4000. Therefore, the device and DHCP server must exchange packets of VLAN 4000.
- When users log in to the new device or devices with no startup configuration files through the console interface, the system prompts the following information: "Auto-Config is working. Before configuring the device, stop Auto-Config. If you perform configurations when Auto-Config is running, the DHCP, routing, DNS, and VTY configurations will be lost. Do you want to stop Auto-Config? [y/n]:".
  - To continue Auto-Config, enter **n**.
  - To stop Auto-Config, enter **y**.

NOTICE

If you do not want to run Auto-Config but enter **n**, the DHCP, routing, DNS, and VTY configurations will be lost after the choice.

2.5 Default Settings for Auto-Config

This section provides the default settings for Auto-Config.

 Copyright © Huawei Technologies Co., Ltd.

Table 2-2 Default settings for Auto-Config

Parameter	Default Setting
Auto-Config function	Enabled

2.6 Configuring Auto-Config on Devices that are on the Same Network Segment with the DHCP Server

The device to be configured that is on the same network segment as the DHCP server can be configured with Auto-Config to automatically load the system software, patch file, and configuration file, realizing remote device deployment.

Pre-configuration Tasks

Before configuring Auto-Config on the device that is on the same network segment as the DHCP server, complete the following tasks:

- Ensure that routes between the DHCP server, file server (FTP/TFTP/SFTP server), and devices are reachable.
- Ensure that no startup configuration file exists on the device.

Configuration Procedure

As networking environment requires, Auto-Config, intermediate file, DHCP server, and file server can be configured on different devices in any sequence. After the preceding configuration tasks are complete, the device is powered on to run the Auto-Config process.

2.6.1 Enabling Auto-Config

Context

Auto-Config needs to be enabled when:

- Auto-Config is disabled on the current device. In this case, you can run the **display autoconfig enable** command to check whether Auto-Config is enabled. Auto-Config must be enabled before it runs.
- If the Auto-Config function cannot be automatically recovered after an error occurs in the Auto-Config process, run the **undo autoconfig enable** command to disable the Auto-Config function. You can use the **display autoconfig-status** command to check whether Auto-Config is enabled. When Auto-Config is in stop state (you can run the **display autoconfig-status** command to check the Auto-Config status), enable Auto-Config again.

  NOTE

  - This task is performed on the device with no startup configuration file.
  - By default, Auto-Config is enabled. Therefore, Auto-Config does not need to be performed on the new device.

Auto-Config can be disabled in the following way:

 Copyright © Huawei Technologies Co., Ltd.

- Run the **undo autoconfig enable** command in the system view to disable Auto-Config. When Auto-Config is in stop state (you can run the **display autoconfig-status** command to check the Auto-Config status), enable Auto-Config again.
- Log in to the device through the console interface. If the following information "Auto-Config is working. Before configuring the device, stop Auto-Config. If you perform configurations when Auto-Config is running, the DHCP, routing, DNS, and VTY configurations will be lost. Do you want to stop Auto-Config? [y/n]:" is displayed, enter **y** to stop the Auto-Config process.

Procedure

Step 1 (Optional) Run display autoconfig enable

Check whether Auto-Config is enabled.

Step 2 Run **system-view**

The system view is displayed.

Step 3 Run autoconfig enable

Auto-Config is enabled.

----End

2.6.2 (Optional) Configuring the Intermediate File

Context

Auto-Config preferentially obtains configuration files through the Option 67 parameter. If Option 67 that contains information about the configuration file is not configured on the DHCP server, Auto-Config enables devices to obtain the configuration file (mandatory), system software (optional), and patch file (optional) using the intermediate file.

The two methods to obtain the configuration file are used in the following scenarios:

- Configure Option 67 on the DHCP server to obtain the configuration file is used when fewer devices need to load the same configuration file.
- Use the intermediate file on the file server to obtain the configuration file is used when many devices need to load different configuration files.

The intermediate file is saved on the FTP/TFTP/SFTP server and contains information about mappings from system MAC address or ESN to the system software name, system software version, patch file name, and configuration file name. After obtaining the IP address of the FTP/TFTP/SFTP server, the device downloads the intermediate file from the FTP/TFTP/SFTP server, searches for the system software, system software version, patch file, and configuration file names that match its own MAC address or ESN, and downloads files from the FTP/TFTP/SFTP server based on the obtained names.

You can check the label on the device to obtain the MAC address and ESN.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

If the intermediate file is configured for the Auto-Config process, Option 67 is not required in configuring the DHCP server.

Procedure

You can configure the intermediate file based on the MAC address or ESN of the device and the required system software, patch file, and configuration file names. The procedure is as follows:

1. Create a file and name the file **arnet.ini**.
2. Configure the intermediate file. For example, if the MAC address of a device is 0018-82C5-AA89, the ESN is 9300070123456789, the version file name is **auto_V200R010.cc**, the version is V200R010, the patch file is **auto_V200R010.pat**, and the configuration file is **auto_V200R010.cfg**, the contents of the intermediate file **arnet.ini** are as follows:

```
MAC=0018-82C5-
AA89;ESN=9300070123456789;vrpfile=auto_V200R010.cc;vrpver=V200R010;patchfile=auto_V200R010.p
at;cfgfile=auto_V200R010.cfg;
```

NOTE

- If multiple devices are configured, each row in the intermediate file records configuration information of a device. A maximum of 1,000 devices are allowed to use the intermediate file to realize Auto-Config.
- When configuring the intermediate file, enter either of the MAC address and ESN. The configuration file is mandatory, and the version file and patch file are optional. The three files can be configured in any sequence.
- The version file name and system software version must be available in the intermediate file, and version ID in the system software name must be the same as that in the intermediate file. vrpver information must be included in the vrpfile information.

2.6.3 Configuring the DHCP Server

Context

Before powering on the devices that need to run Auto-Config, configure the DHCP server and file server; otherwise, the devices cannot obtain configuration files.

NOTE

- The DHCP server must be configured with Option parameters.
- A router is used as an example to describe the procedure for configuring the DHCP server. When the router functions as the DHCP server, configure the DHCP server according to DHCP Configuration. The following example describes the procedure for configuring the DHCP server based on the global address pool.
- After the Auto-Config configuration is complete, delete Auto-Config configuration on the DHCP server to prevent the configuration information from affecting other configurations.

Procedure

Step 1 Run **system-view**

 Copyright © Huawei Technologies Co., Ltd.

The system view is displayed.

Step 2 Run **dhcp enable**

DHCP is enabled.

Step 3 Run **interface** *interface-type interface-number*

The interface view is displayed.

Step 4 Run **ip address** *ip-address* { *mask* | *mask-length* }

An IP address is assigned to the interface.

Step 5 Run **dhcp select global**

The interface is configured to use the global address pool.

Step 6 Run **quit**

Return to the system view.

Step 7 Run **ip pool** *ip-pool-name*

The global address pool is created and the global address pool view is displayed.

By default, no global address pool is created on the device.

Step 8 Run **network** *ip-address* [**mask** { *mask* | *mask-length* }]

The range of IP addresses that can be allocated dynamically in the global address pool is specified.

NOTE

- To prevent IP address conflicts, the configured IP addresses must be different from the IP addresses configured in the configuration files.
- The DHCP server must have IP addresses to assign to devices.

Step 9 Run **gateway-list** *ip-address* &<1-8>

The egress gateway address for DHCP clients is specified.

Step 10 Run **option** *code* [**sub-option** *sub-code*] { **ascii** *ascii-string* | **hex** *hex-string* | **cipher** *cipher-string* | **ip-address** *ip-address* &<1-8> }URL=URL_INFO;URL=http://192.168.1.40:80/acs;username=USERNAME;password=PASSWORD;vrpfile=VRPFILENAME;vrpver=VRPVERSION;patchfile=PATCHFILENAME;Example:vrpfile=auto_V200R010.cc;vrpver=V200R010;patchfile=auto_V200R010.pat;

Option parameters are configured for the DHCP server.

NOTE

When the password is contained in option, the **ascii** or **hex** type is insecure. Set the option type to **cipher**. A secure password should contain at least two types of the following: lowercase letters, uppercase letters, number, and special characters. In addition, the password must consist of six or more than six characters.

If Option 67 is not configured, Auto-Config enables devices to load configuration files using the intermediate file. For details about how to edit the intermediate file, see "**2.6.2 (Optional) Configuring the Intermediate File**".

 Copyright © Huawei Technologies Co., Ltd.

Table 2-3 shows DHCP Option parameters used in Auto-Config.

Table 2-3 DHCP Option parameters

Option	Description
Option 43	Information about the ACS server: • sub-option 1: ACS URL. Format: For example: • sub-option 2: ACS user name and password. Format: **NOTE** The router cannot function as the ACS server. For details about ACS configurations, see corresponding manuals.
Option 67	Name of the configuration file assigned to DHCP clients.
Option 141	FTP/SFTP user name assigned to DHCP clients.
Option 142	FTP/SFTP password assigned to DHCP clients.
Option 143	FTP server IP address assigned to DHCP clients.
Option 145	Information about the non-configuration file assigned to DHCP clients, for example: information about the system software, version ID, and patch file. Format: **NOTE** • vrpver information must be included in the vrpfile information.
Option 146	User-defined settings, including file deletion policy used when memory space is insufficient and delay in activating the configuration file. Format: • opervalue = 0: indicates that no system software will be deleted from the file system when the space is insufficient. opervalue=1: indicates that system software will be deleted from the file system when the space is insufficient. By default, no file will be deleted from the file system when the space is insufficient. • delaytime: specifies the delay in restarting a device after a configuration file is downloaded to the device, in seconds. By default, the delay is 0 seconds. **NOTE** The maximum delay in restarting a device is 1 day, namely, 86400 seconds. If the configured delay exceeds 1 day, the delay is calculated as 1 day.

 Copyright © Huawei Technologies Co., Ltd.

Option	Description
Option 147	Authentication information. Option 147 is optional. If Option 147 is required, it must be configured as AutoConfig.

Option 148	Agile Controller-Branch's IP address and port number assigned to DHCP clients.
	Option 148 is in the following format:
	`agilemode=AGILEMODE;agilemanage-mode=AGILEMANAGE-MODE;agilemanage-domain=AGILEMANAGE-DOMAIN;agilemanage-port=AGILEMANAGE-PORT;`
	• agilemode: indicates the agile mode. agilemode=tradition: indicates the traditional mode.
	• agilemanage-mode: indicates that the agilemanage-domain field is an IP address or a domain name. agilemanage-mode=ip: indicates that the agilemanage-domain field is an IP address. agilemanage-mode=domain: indicates that the agilemanage-domain field is a domain name.
	• agilemanage-domain: indicates an IP address in case of agilemanage-mode=ip or indicates a domain name in case of agilemanage-mode=domain.
	• agilemanage-port: indicates the Agile Controller-Branch's port number assigned to DHCP clients.
	For example, in the Cloud VPN scenario, if the Agile Controller-Branch's IP address and port number assigned to DHCP clients are 10.17.15.84 and 10020, Option 148 is as follows:
	`agilemode=tradition;agilemanage-mode=ip;agilemanage-domain=10.17.15.84;agilemanage-port=10020;`

Option 149	SFTP server IP address and port number assigned to DHCP clients. For example, if the SFTP server IP address is 10.10.10.1 and port number is 22, the Option 149 field is: option 149 ascii ipaddr=10.10.10.1;port=22.
Option 150	TFTP server IP address assigned to DHCP clients.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- Option 150 enables DHCP clients to directly obtain the TFTP server IP address.
- Options 141, 142, and 143 enable DHCP clients to obtain the FTP user name, FTP password, and FTP server address.
- Options 141, 142, and 149 enable DHCP clients to obtain the SFTP user name, SFTP password, and SFTP server IP address and port number.
- When multiple types of Option parameters are set for a DHCP server, the file servers are selected as follows: SFTP -> FTP ->TFTP.
- The file server user name and password obtained by the device to be configured are only used for Auto-Config deployment. The device to be configured does not save the file server user name and password.

----End

2.6.4 Configuring the File Server

Context

NOTE

- If the FTP server is used, the FTP server IP address must be the same as the value of Option 143 configured on the DHCP server. If the TFTP server is used, the TFTP server IP address must be the same as the value of Option 150 configured on the DHCP server. If the SFTP server is used, the SFTP server IP address must be the same as the value of Option 149 configured on the DHCP server.
- The SFTP server is recommended.
- The file server can be the router or a PC. In the following example, a router functions as an SFTP server.

Procedure

Step 1 Enable SFTP. For details, see **11.4 Local File Management**-**11.4.4 Managing Files When the Device Functions as an SFTP Server**-**Set SFTP server parameters.** in *Huawei AR Series Access Routers Configuration Guide-File Management*.

Step 2 Configure the VTY user interface for SSH users, SSH user name, authentication mode, service type and root directory that can be accessed. For details, see **11.4 Local File Management**-**11.4.4 Managing Files When the Device Functions as an SFTP Server**-**Configure the VTY user interface for SSH users to log in to the device.** and **Configure SSH user information.** in *Huawei AR Series Access Routers Configuration Guide-File Management*.

NOTE

Currently, the device supports only password authentication for file access through SFTP.

Step 3 Run **interface** *interface-type interface-number*

The interface view is displayed.

Step 4 Run **ip address** *ip-address* { *mask* | *mask-length* }

The IP address of the SFTP server is configured.

----End

 Copyright © Huawei Technologies Co., Ltd.

Follow-up Procedure

After the file server is configured, place the intermediate file (optional), system software (optional), patch file (optional), and configuration file (mandatory) to the working directory of the file server.

NOTE

- When uploading files, ensure that there is sufficient space in the directory.
- If a PC functions as the file server, copy files to the working directory of the PC (working directory of the file server needs to be specified).
- If the router functions as the file server, upload files to the working directory of the file server using a file client program.
- To ensure file server security, you are advised to configure a unique file server user name and set the right to read-only to prevent the file server from being modified by unauthorized users. After the Auto-Config process is complete, disable the file server function.

2.6.5 Powering on the Device to Start Auto-Config

After preceding configurations are complete, the device is powered on or restarted. The Auto-Config process runs automatically.

2.6.6 Verifying the Configuration

Procedure

- Run the **display ip pool** { **interface** *interface-pool-name* | **name** *ip-pool-name* } **used** command to check the IP addresses that the DHCP server assigns to devices to be configured.
- Run the **display autoconfig-status** command to check the Auto-Config running status.
- Run the **display startup** command to check the startup configuration file, system software, and patch file.

----End

2.7 Configuring Auto-Config Across Different Network Segments

The device that is on a different network segment than the DHCP server can have Auto-Config configured to automatically load the system software, patch file, and configuration file for remote device deployment.

Pre-configuration Tasks

Before configuring Auto-Config on the device that is on a different network segment than the DHCP server, complete the following tasks:

- Ensure that routes between the DHCP server, DHCP relay, file server (FTP/TFTP/SFTP server), and device are reachable.

 Copyright © Huawei Technologies Co., Ltd.

- Ensure that no startup configuration file exists on the device.

Configuration Procedure

As networking environment requires, Auto-Config, intermediate file, DHCP Server, DHCP Relay, and file server can be configured on different devices in any sequence. After the preceding configuration tasks are complete, the device is powered on to run the Auto-Config process.

2.7.1 Enabling Auto-Config

Context

Auto-Config needs to be enabled when:

- Auto-Config is disabled on the current device. In this case, you can run the **display autoconfig enable** command to check whether Auto-Config is enabled. Auto-Config must be enabled before it runs.
- If the Auto-Config function cannot be automatically recovered after an error occurs in the Auto-Config process, run the **undo autoconfig enable** command to disable the Auto-Config function. You can use the **display autoconfig-status** command to check whether Auto-Config is enabled. When Auto-Config is in stop state (you can run the **display autoconfig-status** command to check the Auto-Config status), enable Auto-Config again.

  NOTE

  - This task is performed on the device with no startup configuration file.
  - By default, Auto-Config is enabled. Therefore, Auto-Config does not need to be performed on the new device.

Auto-Config can be disabled in the following way:

- Run the **undo autoconfig enable** command in the system view to disable Auto-Config. When Auto-Config is in stop state (you can run the **display autoconfig-status** command to check the Auto-Config status), enable Auto-Config again.
- Log in to the device through the console interface. If the following information "Auto-Config is working. Before configuring the device, stop Auto-Config. If you perform configurations when Auto-Config is running, the DHCP, routing, DNS, and VTY configurations will be lost. Do you want to stop Auto-Config? [y/n]:" is displayed, enter **y** to stop the Auto-Config process.

Procedure

Step 1 (Optional) Run display autoconfig enable

Check whether Auto-Config is enabled.

Step 2 Run **system-view**

The system view is displayed.

Step 3 Run autoconfig enable

 Copyright © Huawei Technologies Co., Ltd.

Auto-Config is enabled.

----End

2.7.2 (Optional) Configuring the Intermediate File

Context

Auto-Config preferentially obtains configuration files through the Option 67 parameter. If Option 67 that contains information about the configuration file is not configured on the DHCP server, Auto-Config enables devices to obtain the configuration file (mandatory), system software (optional), and patch file (optional) using the intermediate file.

The two methods to obtain the configuration file are used in the following scenarios:

- Configure Option 67 on the DHCP server to obtain the configuration file is used when fewer devices need to load the same configuration file.
- Use the intermediate file on the file server to obtain the configuration file is used when many devices need to load different configuration files.

The intermediate file is saved on the FTP/TFTP/SFTP server and contains information about mappings from system MAC address or ESN to the system software name, system software version, patch file name, and configuration file name. After obtaining the IP address of the FTP/TFTP/SFTP server, the device downloads the intermediate file from the FTP/TFTP/SFTP server, searches for the system software, system software version, patch file, and configuration file names that match its own MAC address or ESN, and downloads files from the FTP/TFTP/SFTP server based on the obtained names.

You can check the label on the device to obtain the MAC address and ESN.

NOTE

If the intermediate file is configured for the Auto-Config process, Option 67 is not required in configuring the DHCP server.

Procedure

You can configure the intermediate file based on the MAC address or ESN of the device and the required system software, patch file, and configuration file names. The procedure is as follows:

1. Create a file and name the file **arnet.ini**.
2. Configure the intermediate file. For example, if the MAC address of a device is 0018-82C5-AA89, the ESN is 9300070123456789, the version file name is **auto_V200R010.cc**, the version is V200R010, the patch file is **auto_V200R010.pat**, and the configuration file is **auto_V200R010.cfg**, the contents of the intermediate file **arnet.ini** are as follows:

```
MAC=0018-82C5-
AA89;ESN=9300070123456789;vrpfile=auto_V200R010.cc;vrpver=V200R010;patchfile=auto_V200R010.p
at;cfgfile=auto_V200R010.cfg;
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- If multiple devices are configured, each row in the intermediate file records configuration information of a device. A maximum of 1,000 devices are allowed to use the intermediate file to realize Auto-Config.
- When configuring the intermediate file, enter either of the MAC address and ESN. The configuration file is mandatory, and the version file and patch file are optional. The three files can be configured in any sequence.
- The version file name and system software version must be available in the intermediate file, and version ID in the system software name must be the same as that in the intermediate file. vrpver information must be included in the vrpfile information.

2.7.3 Configuring the DHCP Server

Context

Before powering on the devices that need to run Auto-Config, configure the DHCP server and file server; otherwise, the devices cannot obtain configuration files.

NOTE

- The DHCP server must be configured with Option parameters.
- A router is used as an example to describe the procedure for configuring the DHCP server. When the router functions as the DHCP server, configure the DHCP server according to DHCP Configuration. The following example describes the procedure for configuring the DHCP server based on the global address pool.
- After the Auto-Config configuration is complete, delete Auto-Config configuration on the DHCP server to prevent the configuration information from affecting other configurations.

Procedure

Step 1 Run **system-view**

The system view is displayed.

Step 2 Run **dhcp enable**

DHCP is enabled.

Step 3 Run **interface** *interface-type interface-number*

The interface view is displayed.

Step 4 Run **ip address** *ip-address* { *mask* | *mask-length* }

An IP address is assigned to the interface.

Step 5 Run **dhcp select global**

The interface is configured to use the global address pool.

Step 6 Run **quit**

Return to the system view.

Step 7 Run **ip pool** *ip-pool-name*

 Copyright © Huawei Technologies Co., Ltd.

The global address pool is created and the global address pool view is displayed.

By default, no global address pool is created on the device.

Step 8 Run **network** *ip-address* [**mask** { *mask* | *mask-length* }]

The range of IP addresses that can be allocated dynamically in the global address pool is specified.

NOTE

- To prevent IP address conflicts, the configured IP addresses must be different from the IP addresses configured in the configuration files.
- The DHCP server must have IP addresses to assign to devices.

Step 9 Run **gateway-list** *ip-address* &<1-8>

The egress gateway address for DHCP clients is specified.

Step 10 Run **option** *code* [**sub-option** *sub-code*] { **ascii** *ascii-string* | **hex** *hex-string* | **cipher** *cipher-string* | **ip-address** *ip-address* &<1-8> }URL=URL_INFO;URL=http://192.168.1.40:80/acs;username=USERNAME;password=PASSWORD;vrpfile=VRPFILENAME;vrpver=VRPVERSION;patchfile=PATCHFILENAME;Example:vrpfile=auto_V200R010.cc;vrpver=V200R010;patchfile=auto_V200R010.pat;

Option parameters are configured for the DHCP server.

NOTE

When the password is contained in option, the **ascii** or **hex** type is insecure. Set the option type to **cipher**. A secure password should contain at least two types of the following: lowercase letters, uppercase letters, number, and special characters. In addition, the password must consist of six or more than six characters.

If Option 67 is not configured, Auto-Config enables devices to load configuration files using the intermediate file. For details about how to edit the intermediate file, see "**2.7.2 (Optional) Configuring the Intermediate File**".

Table 2-4 shows DHCP Option parameters used in Auto-Config.

Table 2-4 DHCP Option parameters

Option	Description
Option 43	Information about the ACS server: • sub-option 1: ACS URL. Format: For example: • sub-option 2: ACS user name and password. Format: **NOTE** The router cannot function as the ACS server. For details about ACS configurations, see corresponding manuals.
Option 67	Name of the configuration file assigned to DHCP clients.
Option 141	FTP/SFTP user name assigned to DHCP clients.

 Copyright © Huawei Technologies Co., Ltd.

Option	Description
Option 142	FTP/SFTP password assigned to DHCP clients.
Option 143	FTP server IP address assigned to DHCP clients.
Option 145	Information about the non-configuration file assigned to DHCP clients, for example: information about the system software, version ID, and patch file. Format: **NOTE** • vrpver information must be included in the vrpfile information.
Option 146	User-defined settings, including file deletion policy used when memory space is insufficient and delay in activating the configuration file. Format: • opervalue = 0: indicates that no system software will be deleted from the file system when the space is insufficient. opervalue=1: indicates that system software will be deleted from the file system when the space is insufficient. By default, no file will be deleted from the file system when the space is insufficient. • delaytime: specifies the delay in restarting a device after a configuration file is downloaded to the device, in seconds. By default, the delay is 0 seconds. **NOTE** The maximum delay in restarting a device is 1 day, namely, 86400 seconds. If the configured delay exceeds 1 day, the delay is calculated as 1 day.
Option 147	Authentication information. Option 147 is optional. If Option 147 is required, it must be configured as AutoConfig.

 Copyright © Huawei Technologies Co., Ltd.

Option	Description

Option 148	Agile Controller-Branch's IP address and port number assigned to DHCP clients.
	Option 148 is in the following format:
	agilemode=AGILEMODE;agilemanage-mode=AGILEMANAGE-MODE;agilemanage-domain=AGILEMANAGE-DOMAIN;agilemanage-port=AGILEMANAGE-PORT;
	• agilemode: indicates the agile mode. agilemode=tradition: indicates the traditional mode.
	• agilemanage-mode: indicates that the agilemanage-domain field is an IP address or a domain name. agilemanage-mode=ip: indicates that the agilemanage-domain field is an IP address. agilemanage-mode=domain: indicates that the agilemanage-domain field is a domain name.
	• agilemanage-domain: indicates an IP address in case of agilemanage-mode=ip or indicates a domain name in case of agilemanage-mode=domain.
	• agilemanage-port: indicates the Agile Controller-Branch's port number assigned to DHCP clients.
	For example, in the Cloud VPN scenario, if the Agile Controller-Branch's IP address and port number assigned to DHCP clients are 10.17.15.84 and 10020, Option 148 is as follows:
	agilemode=tradition;agilemanage-mode=ip;agilemanage-domain=10.17.15.84;agilemanage-port=10020;

Option 149	SFTP server IP address and port number assigned to DHCP clients. For example, if the SFTP server IP address is 10.10.10.1 and port number is 22, the Option 149 field is: option 149 ascii ipaddr=10.10.10.1;port=22.
Option 150	TFTP server IP address assigned to DHCP clients.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- Option 150 enables DHCP clients to directly obtain the TFTP server IP address.
- Options 141, 142, and 143 enable DHCP clients to obtain the FTP user name, FTP password, and FTP server address.
- Options 141, 142, and 149 enable DHCP clients to obtain the SFTP user name, SFTP password, and SFTP server IP address and port number.
- When multiple types of Option parameters are set for a DHCP server, the file servers are selected as follows: SFTP -> FTP ->TFTP.
- The file server user name and password obtained by the device to be configured are only used for Auto-Config deployment. The device to be configured does not save the file server user name and password.

----End

2.7.4 Configuring the DHCP Relay Function

Context

If the device to be configured is on a different segment than the DHCP server, the DHCP relay function needs to be configured to enable the device to obtain configuration information such as IP addresses from the global address pool of the DHCP server.

A maximum of 16 DHCP relay agents can be configured between the DHCP client and server.

NOTE

- This section takes the router as an example to describe the procedure for configuring the DHCP relay function.
- After the Auto-Config deployment is complete, delete the DHCP relay configuration to ensure DHCP relay security.

Procedure

Step 1 Run **system-view**

The system view is displayed.

Step 2 Run **dhcp enable**

DHCP is enabled.

Step 3 Run **interface** *interface-type interface-number*

The interface view is displayed.

Step 4 Run **ip address** *ip-address* { *mask* | *mask-length* }

An IP address is assigned to the interface.

NOTE

When configuring an egress gateway address for the IP address pool on a DHCP server, ensure that this egress gateway address is the same as the IP address of the DHCP relay agent.

 Copyright © Huawei Technologies Co., Ltd.

Step 5 Run **dhcp select relay**

The DHCP relay function is enabled on an interface.

Step 6 Run **quit**

Return to the system view.

Step 7 You can configure the DHCP server IP address on the DHCP relay agent in either of the two following ways:

- Configure the DHCP server IP address directly on the interface. This method can be used when the DHCP relay agent serves only one DHCP server and a few devices need to be configured with Auto-Config on a small network.
  a. Run **interface** *interface-type interface-number*

     The interface view is displayed.
  b. Run **dhcp relay server-ip** *ip-address*

     The DHCP server IP address is configured on the DHCP relay agent.
- Bind DHCP servers to a DHCP server group. This method can be used when the DHCP relay agent serves multiple DHCP servers and many devices need to be configured with Auto-Config on a large network.
  a. Run **dhcp server group** *group-name*

     A DHCP server group is created and the DHCP server group view is displayed.

     A maximum of 64 DHCP server groups can be configured globally.
  b. Run **dhcp-server** *ip-address* [*ip-address-index*]

     DHCP servers are added to a DHCP server group.

     A maximum of 8 DHCP servers can be added to a DHCP server group.
  c. Run **interface** *interface-type interface-number*

     The interface view is displayed.
  d. Run **dhcp relay server-select** *group-name*

     A DHCP server group is configured on the interface.

----End

2.7.5 Configuring the File Server

Context

NOTE

- If the FTP server is used, the FTP server IP address must be the same as the value of Option 143 configured on the DHCP server. If the TFTP server is used, the TFTP server IP address must be the same as the value of Option 150 configured on the DHCP server. If the SFTP server is used, the SFTP server IP address must be the same as the value of Option 149 configured on the DHCP server.
- The SFTP server is recommended.
- The file server can be the router or a PC. In the following example, a router functions as an SFTP server.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Enable SFTP. For details, see **11.4 Local File Management**-**11.4.4 Managing Files When the Device Functions as an SFTP Server**-**Set SFTP server parameters.** in *Huawei AR Series Access Routers Configuration Guide-File Management*.

Step 2 Configure the VTY user interface for SSH users, SSH user name, authentication mode, service type and root directory that can be accessed. For details, see **11.4 Local File Management-11.4.4 Managing Files When the Device Functions as an SFTP Server**-**Configure the VTY user interface for SSH users to log in to the device.** and **Configure SSH user information.** in *Huawei AR Series Access Routers Configuration Guide-File Management*.

NOTE

Currently, the device supports only password authentication for file access through SFTP.

Step 3 Run **interface** *interface-type interface-number*

The interface view is displayed.

Step 4 Run **ip address** *ip-address* { *mask* | *mask-length* }

The IP address of the SFTP server is configured.

----End

Follow-up Procedure

After the file server is configured, place the intermediate file (optional), system software (optional), patch file (optional), and configuration file (mandatory) to the working directory of the file server.

NOTE

- When uploading files, ensure that there is sufficient space in the directory.
- If a PC functions as the file server, copy files to the working directory of the PC (working directory of the file server needs to be specified).
- If the router functions as the file server, upload files to the working directory of the file server using a file client program.
- To ensure file server security, you are advised to configure a unique file server user name and set the right to read-only to prevent the file server from being modified by unauthorized users. After the Auto-Config process is complete, disable the file server function.

2.7.6 Powering on the Device to Start Auto-Config

After preceding configurations are complete, the device is powered on or restarted. The Auto-Config process runs automatically.

2.7.7 Verifying the Configuration

Procedure

- Run the **display autoconfig-status** command to check the Auto-Config running status.

 Copyright © Huawei Technologies Co., Ltd.

- Run the **display ip pool** { **interface** *interface-pool-name* | **name** *ip-pool-name* } **used** command to check the IP addresses that the DHCP server assigns to devices to be configured.
- Run the **display dhcp relay** { **all** | **interface** *interface-type interface-number* } command to check the DHCP server or DHCP server group on the interface.
- Run the **display dhcp server group** [*group-name*] command to check configuration of the DHCP server group on the DHCP relay agent.
- Run the **display startup** command to check the startup configuration file, system software, and patch file.

----End

2.8 Maintaining Auto-Config

You can monitor the running status of Auto-Config in each phase to ensure that Auto-Config runs normally.

Procedure

Step 1 Five minutes after devices without any configuration file are powered on, check address allocation on the DHCP server to determine whether devices are connected to the network. Run the **display ip pool** { **interface** *interface-pool-name* | **name** *ip-pool-name* } **used** command to check the IP addresses that the DHCP server assigns to devices to be configured.

NOTE

If the device is connected to the network, you can Telnet to the device but do not configure the device.

Step 2 Five minutes after devices obtain IP addresses, check the file transmission log on the file server, or log in to the devices to check whether correct system software, patch files, and configuration files have been downloaded and check the running status of Auto-Config using the **display autoconfig-status** command.

NOTE

- Do not save configuration immediately to a device after the configuration file is downloaded; otherwise, only a temporary configuration file is saved because the configuration has not taken effect.
- If devices fail to obtain the files, the Auto-Config process is suspended. Run the **autoconfig getting-file restart** command to obtain the system software, patch file, and configuration file to resume the Auto-Config process.

Step 3 After the configuration file is downloaded successfully, the device is restarted according to the setting of Option 146.

1. Run the **display autoconfig activating-config delay** command to check the configured delay in restarting the device.
2. Run the **display autoconfig activating-config remanent-time** command to check the remaining delay in restarting the device.

----End

 Copyright © Huawei Technologies Co., Ltd.

2.9 Configuration Examples for Auto-Config

This section provides Auto-Config configuration examples including networking requirements and configuration roadmap.

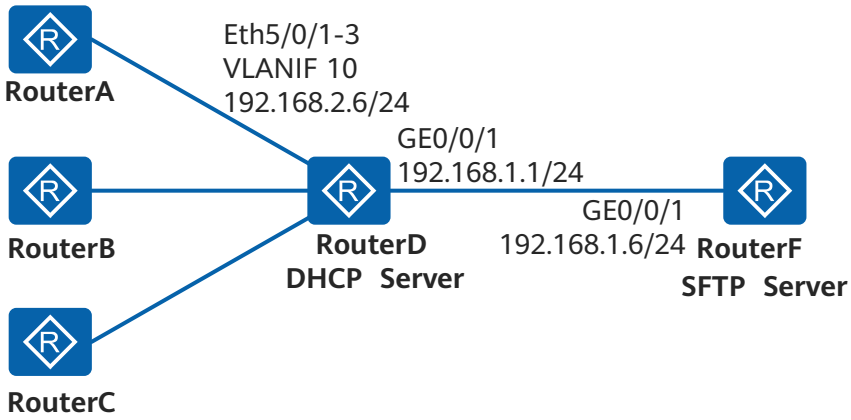
2.9.1 Example for Configuring Auto-Config on the Same Network Segment

Networking Requirements

As shown in **Figure 2-5**, in the network deployment for a residential community, the aggregation device RouterD is connected to new Routers (such as RouterA, RouterB, and RouterC) on each layer of buildings in the residential community.

Users want to load the same system software, patch file, and configuration file on all the Routers on layers. Besides, to save manpower costs and deployment time of many Routers, the Routers are required to be automatically configured with the same configuration.

Figure 2-5 Configuring Auto-Config on the Same Network Segment



Configuration Roadmap

The configuration roadmap is as follows:

1. Directly connect RouterF to RouterD and configure RouterF as the SFTP server. Configure an default route on RouterF so that RouterF can communicate with other device.
2. Place the configuration file, system software, and patch file to be loaded to the working directory of the SFTP server to ensure that RouterA, RouterB, and RouterC can obtain files to be loaded.
3. Configure RouterD as the DHCP server to provide network configurations to RouterA, RouterB, and RouterC. Configure information about the system

 Copyright © Huawei Technologies Co., Ltd.

software, patch file, and configuration file in Option 67 and Option 145 because the same files are to be loaded on all the Routers.

4. Power on RouterA, RouterB, and RouterC, so that the configuration file, system software, and patch file are automatically loaded using auto-config.

NOTE

By default, auto-config is enabled on a Router.

Procedure

Step 1 Configuring RouterF as the SFTP server

Set SFTP server parameters.

```
<Huawei> system-view
[Huawei] sysname SFTP Server
[SFTP Server] rsa local-key-pair create
The key name will be: Host
RSA keys defined for Host already exist.
Confirm to replace them? (y/n)[n]:y
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is less than 2048,
       It will introduce potential security risks.
Input the bits in the modulus[default = 2048]:2048
Generating keys...
.....+++
....+++
.....++++++++
.............++++++++
[SFTP Server] sftp server enable
```

Configuring the VTY user interface for SSH users to log in to the device.

```
[SFTP Server] user-interface vty 0 4
[SFTP Server-ui-vty0-4] authentication-mode aaa
[SFTP Server-ui-vty0-4] protocol inbound all
[SFTP Server-ui-vty0-4] user privilege level 15
[SFTP Server-ui-vty0-4] quit
```

Configuring SSH user information.

```
[SFTP Server] aaa
[SFTP Server-aaa] local-user user password
Please configure the login password (8-128)
It is recommended that the password consist of at least 2 types of characters, i
ncluding lowercase letters, uppercase letters, numerals and special characters.
Please enter password:
Please confirm password:
[SFTP Server-aaa] local-user user privilege level 15
[SFTP Server-aaa] local-user user service-type ssh
[SFTP Server-aaa] local-user user ftp-directory flash:/autoconfig
[SFTP Server-aaa] quit
[SFTP Server] ssh user user authentication-type password
```

Configuring the IP address of the SFTP server.

```
[SFTP Server] interface gigabitethernet 0/0/1
[SFTP Server-GigabitEthernet0/0/1] ip address 192.168.1.6 24
[SFTP Server-GigabitEthernet0/0/1] quit
```

Configuring an default route on SFTP server.

```
[SFTP Server] ip route-static 0.0.0.0 0.0.0.0 192.168.1.1
```

 Copyright © Huawei Technologies Co., Ltd.

Step 2 Upload the system software, configuration file, and patch file to the SFTP server working directory **flash:/autoconfig**. Procedures for uploading the files are not mentioned here

Step 3 Configuring the DHCP server (for example, AR2220)

```
<Huawei> system-view
[Huawei] sysname DHCP Server
[DHCP Server] dhcp enable
[DHCP Server] vlan 10
[DHCP Server-vlan10] quit
[DHCP Server] interface ethernet 5/0/1
[DHCP Server-Ethernet5/0/1] port link-type hybrid
[DHCP Server-Ethernet5/0/1] port hybrid untagged vlan 10
[DHCP Server-Ethernet5/0/1] port hybrid pvid vlan 10
[DHCP Server-Ethernet5/0/1] quit
[DHCP Server] interface ethernet 5/0/2
[DHCP Server-Ethernet5/0/2] port link-type hybrid
[DHCP Server-Ethernet5/0/2] port hybrid untagged vlan 10
[DHCP Server-Ethernet5/0/2] port hybrid pvid vlan 10
[DHCP Server-Ethernet5/0/2] quit
[DHCP Server] interface ethernet 5/0/3
[DHCP Server-Ethernet5/0/3] port link-type hybrid
[DHCP Server-Ethernet5/0/3] port hybrid untagged vlan 10
[DHCP Server-Ethernet5/0/3] port hybrid pvid vlan 10
[DHCP Server-Ethernet5/0/3] quit
[DHCP Server] interface gigabitEthernet 0/0/1
[DHCP Server-GigabitEthernet0/0/1] ip address 192.168.1.1 255.255.255.0
[DHCP Server-GigabitEthernet0/0/1] quit
[DHCP Server] interface vlanif 10
[DHCP Server-Vlanif10] ip address 192.168.2.6 255.255.255.0
[DHCP Server-Vlanif10] dhcp select global
[DHCP Server-Vlanif10] quit
[DHCP Server] ip pool auto-config
[DHCP Server-ip-pool-auto-config] network 192.168.2.0 mask 255.255.255.0
[DHCP Server-ip-pool-auto-config] gateway-list 192.168.2.6
[DHCP Server-ip-pool-auto-config] option 67 ascii ar_V200R010.cfg
[DHCP Server-ip-pool-auto-config] option 141 ascii user
[DHCP Server-ip-pool-auto-config]  option 142 cipher huawei@123
[DHCP Server-ip-pool-auto-config] option 143 ip-address 192.168.1.6
[DHCP Server-ip-pool-auto-config] option 145 ascii
vrpfile=auto_V200R010.cc;vrpver=V200R010;patchfile=ar_V200R010.pat;
[DHCP Server-ip-pool-auto-config] option 149 ascii ipaddr=192.168.1.6;port=22;

[DHCP Server-ip-pool-auto-config] quit
```

Step 4 Power on RouterA, RouterB, and RouterC, and run the Auto-config process

Step 5 Verify the configuration

After auto-config is finished, log in to the Router to be configured and run the **display startup** command to view the system software, configuration file, and patch file for the startup of the Router. RouterA is used as an example.

```
<Huawei> display startup
MainBoard:
  Startup system software:                flash:/ar_V200R010.cc
  Next startup system software:           flash:/ar_V200R010.cc
  Backup system software for next startup:   null
  Startup saved-configuration file:       flash:/ar_V200R010.cfg
  Next startup saved-configuration file:     flash:/ar_V200R010.cfg
  Startup license file:                  null
  Next startup license file:               null
  Startup patch package:                   flash:/ar_V200R010.pat
  Next startup patch package:              flash:/ar_V200R010.pat
  Startup voice-files:                   null
  Next startup voice-files:                null
```

----End

 Copyright © Huawei Technologies Co., Ltd.

Configuration Files

- Configuration file of the SFTP server

```
#
 sysname SFTP Server
#
aaa
 local-user user ftp-directory flash:/autoconfig
 local-user user password cipher %$%$c|-D8KO4/,B[(FR.r!LHg]TK%$%$
 local-user user privilege level 15
 local-user user service-type ssh
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.6 255.255.255.0
#
 sftp server enable
#
ip route-static 0.0.0.0 0.0.0.0 192.168.1.1
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
 user privilege level 15
#
return
```

- Configuration file of the DHCP server

```
#
 sysname DHCP Server
#
vlan batch 10
#
 dhcp enable
#
ip pool auto-config
 gateway-list 192.168.2.6
 network 192.168.2.0 mask 255.255.255.0
 option 67 ascii ar_V200R003C00.cfg
 option 141 ascii user
 option 142 cipher %@%@djZ=#=yW^UB}YAMrrT;ItpY@%@%@
 option 143 ip-address 192.168.1.6
 option 145 ascii vrpfile=auto_V200R010.cc;vrpver=V200R010;patchfile=ar_V200R010.pat;
 option 149 ascii ipaddr=192.168.1.6;port=22;
#
interface Vlanif10
 ip address 192.168.2.6 255.255.255.0
 dhcp select global
#
interface Ethernet5/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet5/0/2
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet5/0/3
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

2.9.2 Example for Configuring Auto-Config on Different Network Segments

Networking Requirements

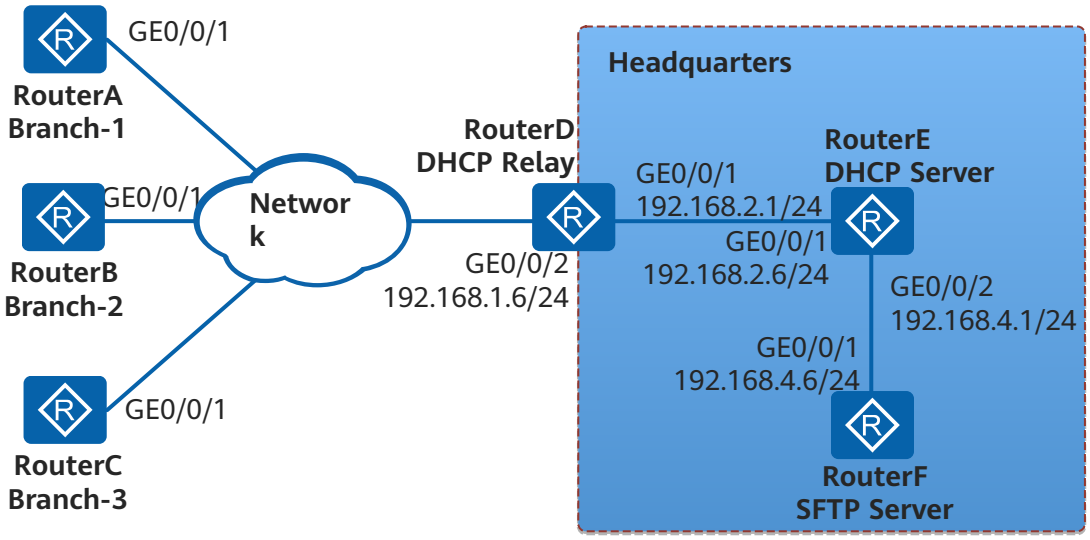
As shown in **Figure 2-6**, in the network deployment for branches of an enterprise, the newly delivered RouterA, RouterB, and RouterC need to be deployed in branches 1, 2, 3 of an enterprise. The three routers connect to GE0/0/2 of RouterD across the transmission network through their GE0/0/1 interfaces respectively. RouterD functions as the egress gateway of the enterprise and is connected to the headquarters across the Layer 3 network through their GE0/0/1 interfaces.

Users want to load same system software and patch files, and different configuration files on RouterA, RouterB, and RouterC. Besides, to save manpower costs, users want the Routers to be automatically configured with different configurations.

Information about RouterA, RouterB, RouterC, and files to be loaded is as follows:

- RouterA: MAC address: 0018-82C5-AA89; ESN: 2102310CXK10B6000183; system software: auto_V200R010.cc; system software version: V200R010, patch file: auto_V200R010.pat; configuration file: auto_RouterA.cfg
- RouterB: MAC address: 0018-82C5-AA90; ESN: 2102310CXK10B6000184; system software: auto_V200R010.cc; system software version: V200R010; patch file: auto_V200R010.pat; configuration file: auto_RouterB.cfg
- RouterC: MAC address: 0018-82C5-AA91; ESN: 2102310CXK10B6000185; system software: auto_V200R010.cc; system software version: V200R010; patch file: auto_V200R010.pat; configuration file: auto_RouterC.cfg.

Figure 2-6 Configuring Auto-Config on Different Network Segments



 Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

The configuration roadmap is as follows:

1. Directly connect RouterF to RouterE and configure RouterF as the SFTP server. Configure an default route on RouterF so that RouterF can communicate with other device.
2. Configure an intermediate file so that RouterA, RouterB, and RouterC can obtain configuration files, system software, and patch files through the intermediate file.
3. Place the intermediate file, configuration files, system software, and patch files to be loaded to the working directory of the SFTP server to ensure that Routers to be configured can obtain files to be loaded.
4. Configure the enterprise gateway RouterD as the DHCP relay agent and configure RouterE in the headquarters as the DHCP server so that the DHCP server can deliver network configurations to Routers to be configured on different network segments.
5. Power on RouterA, RouterB, and RouterC so that configuration files, system software, and patch files are automatically loaded using auto-config.

NOTE

- By default, auto-config is enabled on a Router.

Procedure

Step 1 Configuring RouterF as the SFTP server

Set SFTP server parameters.

```
<Huawei> system-view
[Huawei] sysname SFTP Server
[SFTP Server] rsa local-key-pair create
The key name will be: Host
RSA keys defined for Host already exist.
Confirm to replace them? (y/n)[n]:y
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is less than 2048,
       It will introduce potential security risks.
Input the bits in the modulus[default = 2048]:2048
Generating keys...
.....+++
....+++
.....++++++++
.............++++++++
[SFTP Server] sftp server enable
```

Configuring the VTY user interface for SSH users to log in to the device.

```
[SFTP Server] user-interface vty 0 4
[SFTP Server-ui-vty0-4] authentication-mode aaa
[SFTP Server-ui-vty0-4] protocol inbound all
[SFTP Server-ui-vty0-4] user privilege level 15
[SFTP Server-ui-vty0-4] quit
```

Configuring SSH user information.

```
[SFTP Server] aaa
[SFTP Server-aaa] local-user user password
Please configure the login password (8-128)
It is recommended that the password consist of at least 2 types of characters, i
```

 Copyright © Huawei Technologies Co., Ltd.

```
ncluding lowercase letters, uppercase letters, numerals and special characters.
Please enter password:
Please confirm password:
[SFTP Server-aaa] local-user user privilege level 15
[SFTP Server-aaa] local-user user service-type ssh
[SFTP Server-aaa] local-user user ftp-directory flash:\autoconfig
[SFTP Server-aaa] quit
[SFTP Server] ssh user user authentication-type password
```

Configuring the IP address of the SFTP server.

```
[SFTP Server] interface gigabitethernet 0/0/1
[SFTP Server-GigabitEthernet0/0/1] ip address 192.168.4.6 24
[SFTP Server-GigabitEthernet0/0/1] quit
```

Configuring an default route on SFTP server.

```
[SFTP Server] ip route-static 0.0.0.0 0.0.0.0 192.168.4.1
```

Step 2 Configuring an intermediate file **arnet.ini**

Create a file and name the file **arnet.ini**. The contents and format of the intermediate file are as follows:

```
MAC=0018-82C5-
AA89;ESN=2102310CXK10B6000183;vrpfile=auto_V200R010.cc;vrpver=V200R010;patchfile=auto_V200R010.p
at;cfgfile=auto_RouterA.cfg;
MAC=0018-82C5-
AA90;ESN=2102310CXK10B6000184;vrpfile=auto_V200R010.cc;vrpver=V200R010;patchfile=auto_V200R010.p
at;cfgfile=auto_RouterB.cfg;
MAC=0018-82C5-
AA91;ESN=2102310CXK10B6000185;vrpfile=auto_V200R010.cc;vrpver=V200R010;patchfile=auto_V200R010.p
at;cfgfile=auto_RouterC.cfg;
```

Step 3 Uploading the intermediate file, system software, configuration file, and patch file to the SFTP server working directory **flash:\autoconfig**. Procedures for upload the files are not mentioned here

Step 4 Configuring RouterD

Configure RouterD as the DHCP relay agent.

```
<Huawei> system-view
[Huawei] sysname DHCP Relay
[DHCP Relay] dhcp enable
[DHCP Relay] interface gigabitethernet 0/0/2
[DHCP Relay-GigabitEthernet0/0/2] ip address 192.168.1.6 255.255.255.0
[DHCP Relay-GigabitEthernet0/0/2] dhcp select relay
[DHCP Relay-GigabitEthernet0/0/2] dhcp relay server-ip 192.168.2.6
[DHCP Relay-GigabitEthernet0/0/2] quit
[DHCP Relay] interface gigabitethernet 0/0/1
[DHCP Relay-GigabitEthernet0/0/1] ip address 192.168.2.1 255.255.255.0
[DHCP Relay-GigabitEthernet0/0/1] quit
[DHCP Relay] ip route-static 192.168.4.0 255.255.255.0 192.168.2.6
```

Step 5 Configuring RouterE

Configure RouterE as the DHCP server.

```
<Huawei> system-view
[Huawei] sysname DHCP Server
[DHCP Server] dhcp enable
[DHCP Server] interface GigabitEthernet 0/0/1
[DHCP Server-GigabitEthernet0/0/1] ip address 192.168.2.6 255.255.255.0
[DHCP Server-GigabitEthernet0/0/1] dhcp select global
[DHCP Server-GigabitEthernet0/0/1] quit
[DHCP Server] interface GigabitEthernet 0/0/2
[DHCP Server-GigabitEthernet0/0/2] ip address 192.168.4.1 255.255.255.0
[DHCP Server-GigabitEthernet0/0/2] quit
[DHCP Server] ip pool auto-config
[DHCP Server-ip-pool-auto-config] network 192.168.1.0 mask 255.255.255.0
[DHCP Server-ip-pool-auto-config] gateway-list 192.168.1.6
[DHCP Server-ip-pool-auto-config] option 141 ascii user
```

 Copyright © Huawei Technologies Co., Ltd.

```
[DHCP Server-ip-pool-auto-config] option 142 cipher huawei@123
[DHCP Server-ip-pool-auto-config] option 143 ip-address 192.168.4.6
[DHCP Server-ip-pool-auto-config] option 146 ascii opervalue=1;delaytime=0;netfile=arnet.ini;
[DHCP Server-ip-pool-auto-config] quit
[DHCP Server] ip route-static 192.168.1.0 255.255.255.0 192.168.2.1
```

Step 6 Powering on RouterA, RouterB, and RouterC, and run the Auto-config process

Step 7 Verifying the configuration

After auto-config is finished, log in to the Router to be configured and run the **display startup** command to view the system software, configuration file, and patch file for the startup of the Router. RouterC is used as an example.

```
<Huawei> display startup
MainBoard:
  Startup system software:                flash:/auto_V200R010.cc
  Next startup system software:           flash:/auto_V200R010.cc
  Backup system software for next startup:   null
  Startup saved-configuration file:       flash:/auto_RouterC.cfg
  Next startup saved-configuration file:     flash:/auto_RouterC.cfg
  Startup license file:                   null
  Next startup license file:              null
  Startup patch package:                  flash:/auto_V200R010.pat
  Next startup patch package:             flash:/auto_V200R010.pat
  Startup voice-files:                    null
  Next startup voice-files:               null
```

----End

Configuration Files

- Configuration file of the SFTP server

```
#
 sysname SFTP Server
#
aaa
 local-user user ftp-directory flash:\autoconfig
 local-user user password cipher %$%$c|-D8KO4/,B[(FR.r!LHg]TK%$%$
 local-user user privilege level 15
 local-user user service-type ssh
#
interface GigabitEthernet0/0/1
 ip address 192.168.4.6 255.255.255.0
#
 sftp server enable
#
ip route-static 0.0.0.0 0.0.0.0 192.168.4.1
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
 user privilege level 15
#
return
```

- Configuration file of the DHCP relay agent

```
#
 sysname DHCP Relay
#
 dhcp enable
#
interface GigabitEthernet0/0/1
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 192.168.1.6 255.255.255.0
 dhcp select relay
```

 Copyright © Huawei Technologies Co., Ltd.

```
 dhcp relay server-ip 192.168.2.6
#
ip route-static 192.168.4.0 255.255.255.0 192.168.2.6
#
return
```

- Configuration file of the DHCP server

```
#
 sysname DHCP Server
#
 dhcp enable
#
ip pool auto-config
 gateway-list 192.168.1.6
 network 192.168.1.0 mask 255.255.255.0
 option 141 ascii user
 option 142 cipher %@%@djZ=#=yW^UB}YAMrrT;ItpY@%@%@
 option 143 ip-address 192.168.4.6
 option 146 ascii opervalue=1;delaytime=0;netfile=arnet.ini;
#
interface GigabitEthernet0/0/1
 ip address 192.168.2.6 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/2
 ip address 192.168.4.1 255.255.255.0
#
ip route-static 192.168.1.0 255.255.255.0 192.168.2.1
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

3 Auto-Start Configuration

About This Chapter

Auto-Start enables a device to automatically load version files including the system software, patch file, and configuration file, simplifying configuration and reducing site deployment costs.

3.1 Overview of Auto-Start
This section describes the definition and purpose of Auto-Start.

3.2 Application Scenarios for Auto-Start
This section describes the application scenarios for Auto-Start.

3.3 Understanding Auto-Start
This section describes how Auto-Start is implemented.

3.4 Licensing Requirements and Limitations for Auto-Start
This section provides licensing requirements and limitations for Auto-Start.

3.5 Default Settings for Auto-Start
This section describes the default settings for Auto-Start.

3.6 Configuring Auto-Start
This chapter describes how to configure Auto-Start.

3.7 Maintaining Auto-Start
You can monitor the running status of Auto-Start in each phase to ensure that Auto-Start runs normally.

3.8 Configuration Examples for Auto-Start
This section provides Auto-Start configuration examples, including the networking requirements, configuration roadmap, and configuration procedure.

3.1 Overview of Auto-Start

This section describes the definition and purpose of Auto-Start.

 Copyright © Huawei Technologies Co., Ltd.

Definition

The Auto-Start function allows a device to automatically load version files after it is powered on and starts.

Purpose

Auto-Config and Auto-Start allow devices to automatically load version files to implement batch site deployment and quick remote deployment of devices to be connected to the network. The two functions reduce labor costs and improve device deployment efficiency.

The differences between the two functions are as follows:

- Auto-Config is generally used for automatic site deployment on LANs. After being installed and powered on at a site, devices obtain IP addresses and configuration information related to the file server through the DHCP server deployed on the LAN. The devices then automatically obtain version files from a specified file server based on the configuration information and load the files to complete site deployment.
- Auto-Start is generally used for automatic site deployment across LANs. Devices load site deployment configurations including IP addresses and configuration information related to the file server in advance using customized factory settings or USB flash drives. After being installed and powered on at a site, the devices directly set up connections to the file server, automatically obtain version files from the file server and load the files to complete site deployment.

Related Documents

Video:**Auto-Start Feature of Huawei AR Routers**

3.2 Application Scenarios for Auto-Start

This section describes the application scenarios for Auto-Start.

Auto-Start Deployment

You can configure Auto-Start based on the networking shown in **Figure 3-1**, and store the intermediate file (mandatory) and at least one of the configuration file, system software, and patch file on the FTP/SFTP server. Software commissioning engineers uniformly configure management IP addresses and file server parameters, and enable Auto-Start on devices. Installation personnel then deploy these devices to different sites. As long as these devices have reachable routes to the file server, the devices use Auto-Start to automatically obtain version files from the FTP/SFTP server and load configuration files, system software, and patch files after being powered on.

You can also use the customization mode, add the devices' IP addresses and file server parameters to factory settings, and enable Auto-Start. After being delivered, installed at sites, and powered on, the devices start the Auto-Start process for site deployment.

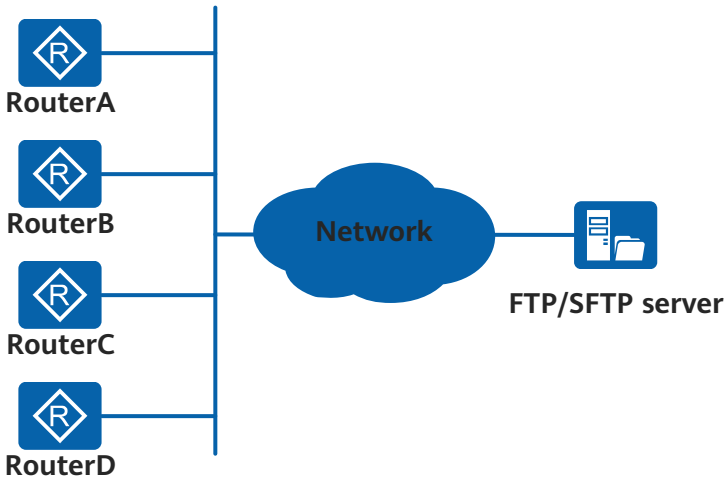
You can also use Auto-Start to upgrade devices in the future. You only need to save files (intermediate file, system software, patch file, and configuration file)

 Copyright © Huawei Technologies Co., Ltd.

required for the upgrade to the file server, reconfigure file server parameters, and restart the devices. The devices then use Auto-Start to automatically load new version files. If file server parameters remain unchanged and are saved to the configuration file, you do not need to reconfigure the parameters.

Auto-Start allows devices to rapidly and automatically load version files in batches, so that professional software commissioning engineers do not need to go to sites. Auto-Start reduces site deployment costs, simplifies site deployment process, and improves device deployment efficiency.

Figure 3-1 Auto-Start networking



3.3 Understanding Auto-Start

This section describes how Auto-Start is implemented.

Auto-Start Principles

Before using Auto-Start for site deployment, make an intermediate file and save it to a specified directory on the file server. Save version files to be loaded to the specified directory on the file server. After configuring an IP address and file server parameters on a device, enable Auto-Start. The device then automatically downloads and loads version files based on the intermediate file after the start.

The intermediate file contains the mapping between the device's MAC address + equipment serial number (ESN) and the system software, version, patch file, and configuration file. A device uses the file server's IP address, a user name, and a password to set up a connection with the file server, downloads and parses the intermediate file. After successfully parsing the intermediate file, the device downloads corresponding version files from the file server and loads the files. For details about how to make the intermediate file, see **3.6.1 Making the Intermediate File**.

Site deployment files consist of mandatory and optional files.

- Mandatory file
  - Intermediate file: The file name must be **arstart.ini**.
- Optional file

 Copyright © Huawei Technologies Co., Ltd.

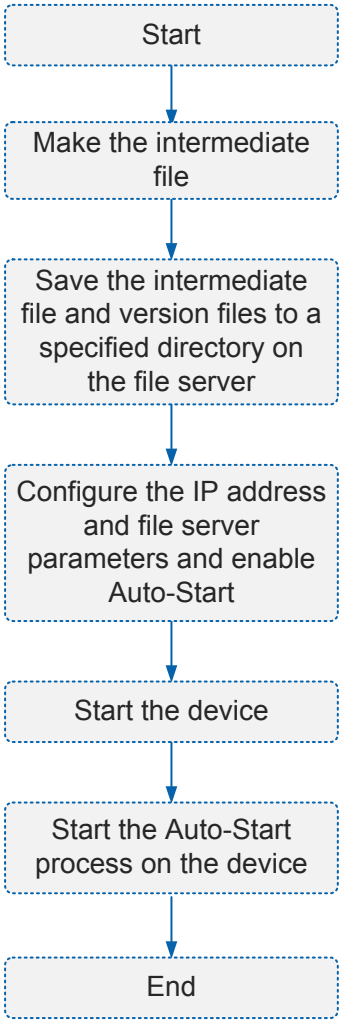
- System software: The file name extension is .cc or .zip.
- Patch file: The file name extension is .pat.
- Configuration file: The file name extension is .cfg or .zip.

You can select at least one optional file for site deployment using Auto-Start.

Site Deployment Process Using Auto-Start

Figure 3-2 shows the site deployment process using Auto-Start.

Figure 3-2 Site deployment process using Auto-Start



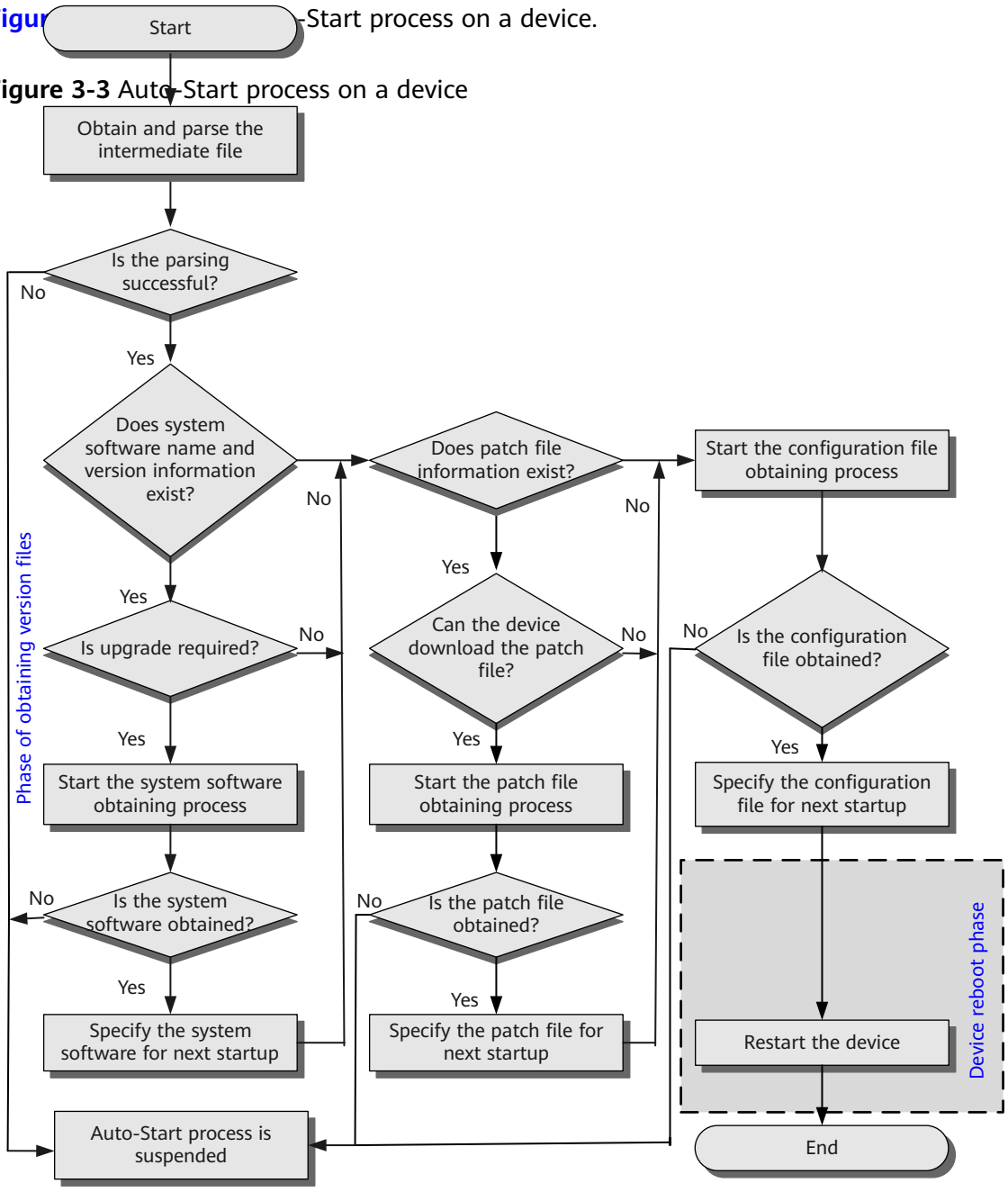
1. Make an intermediate file.
2. Save the intermediate file and version files to a specified directory on the file server.
3. Configure the device's IP address and file server parameters.
4. Enable Auto-Start.
5. The device starts the Auto-Start process.
6. The site deployment process using Auto-Start ends.

 Copyright © Huawei Technologies Co., Ltd.

Auto-Start Process on a Device

Figur Start process on a device.

Figure 3-3 Auto-Start process on a device



1. The device connects to the file server to obtain and parse the intermediate file.
   - If the device successfully parses the file, go to step 2.
   - If the device fails to obtain or parse the file, the site deployment fails.
2. The device obtains site deployment files from the file server and saves the files to a specified storage medium according to description in the intermediate file.
   - If the device successfully obtains the files, go to step 3.
   - If the device fails to obtain the files, the site deployment fails.

 Copyright © Huawei Technologies Co., Ltd.

3. The device specifies the system software, configuration file, and patch file as next startup files.
4. The device restarts.

3.4 Licensing Requirements and Limitations for Auto-Start

This section provides licensing requirements and limitations for Auto-Start.

Involved Network Elements

None

Licensing Requirements

Auto-Start is a basic feature of a router and is not under license control.

Feature Limitations

- The device can be deployed using a USB flash drive, Auto-Config, or Auto-Start. The three deployment modes are mutually exclusive and only one of them can be used at a time.
- The intermediate file contains the mapping between the device's MAC address + ESN and the system software, version, patch file, and configuration file. After connecting to the file server, the device downloads and parses the intermediate file, and downloads corresponding version files from the file server based on the parsing result. Before using Auto-Start, obtain the device's system MAC address and ESN using the following methods:
  - View the barcode label attached to the surface of the device.
  - Log in to the device and run the **display system-mac** (diagnostic view) and **display esn** (All views) commands to view the MAC address and ESN, respectively.

3.5 Default Settings for Auto-Start

This section describes the default settings for Auto-Start.

Table 3-1 Default settings for Auto-Start

Parameter	Default Setting
Auto-Start	Disabled

3.6 Configuring Auto-Start

This chapter describes how to configure Auto-Start.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Process

To configure Auto-Start, perform the following configuration tasks on the file server and device. The tasks can be performed in any sequence. You must complete all the tasks before running Auto-Start on the device.

3.6.1 Making the Intermediate File

This section describes the intermediate file and how to make the file.

Context

An Auto-Start-enabled device parses the intermediate file to obtain information about version files to be downloaded. For details about the Auto-Start process, see **3.3 Understanding Auto-Start**.

The intermediate file must be named **arstart.ini** and saved in an authorized directory on the file server. The file contains the mapping between the device's MAC address + ESN and the system software, version, patch file, and configuration file. The system software, patch file, and configuration file are saved in the authorized directory on the file server. The file name extension of the system software is .cc or .zip, that of the patch file is .pat, and that of the configuration file is .zip or .cfg. After obtaining the file server's IP address, the device downloads the file **arstart.ini** from the file server, parses the file to find names of corresponding system software, version, patch file, and configuration file, and downloads version files from the file server based on the names.

Procedure

Step 1 Create a text file and name it **arstart.ini**.

Step 2 Edit the intermediate file.

Assume that a router's MAC address (**obtaining method**) is 0018-82C5-AA89, ESN (**obtaining method**) is 9300070123456789, system software to be downloaded is auto_V200R007C00.cc, version is V200R007C00, patch file to be downloaded is auto_V200R007C00.pat, and configuration file to be downloaded is auto_V200R007C00.cfg. The contents of the intermediate file **arstart.ini** are as follows:

```
MAC=0018-82C5-
AA89;ESN=9300070123456789;vrpfile=auto_V200R007C00.cc;vrpver=V200R007C00;patchfile=auto_V200R007
C00.pat;cfgfile=auto_V200R007C00.cfg;
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- If multiple devices need to be configured, each line in the intermediate file records configuration information of a device. A maximum of 1,000 devices can use the intermediate file to implement Auto-Start.
- When editing the intermediate file, enter the MAC address and ESN, or either of them. Names of the configuration file, system software, and patch file are optional. Enter at least one file name.
- The MAC address, ESN, version, and names of the system software, patch file, and configuration file can be written in any sequence.
- The MAC address (or ESN), system software name, patch file name, and configuration file name are separated by semicolons (;). The MAC address is in xxxx-xxxx-xxxx-xxxx or xx-xx-xx-xx format. The file name is case-insensitive and does not contain special characters. It is recommended that the file name contain letters, digits, and underscores (_).
- The intermediate file must contain the system software name and version, and the version in the system software name must be the same as the version in the intermediate file. The version information (*vrpver*) must be included in the system software information (*vrpfile*).

----End

3.6.2 Configuring the File Server

This section describes how to configure the file server.

Prerequisites

The file server works properly.

Context

- The file server can be an FTP or SFTP server. An SFTP server is recommended.
- The device or a PC can function as the file server.

Procedure

Configure the file server.

- For details about how to configure the file server as an FTP server, see **11.4.3 Managing Files When the Device Functions as an FTP Server**.
- For details about how to configure the file server as an SFTP server, see **11.4.4 Managing Files When the Device Functions as an SFTP Server**.

Follow-up Procedure

After configuring the file server, save the intermediate file (mandatory) and at least one of the configuration file, system software, and patch file to an authorized directory on the file server.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- Before uploading files to the file server, ensure that the directory has sufficient space to store the files.
- If a PC functions as the file server, directly copy the files to the authorized directory on the PC (the authorized directory on the file server needs to be specified).
- If the device functions as the file server, use third-party software on a PC to upload the files to the authorized directory on the file server.
- To ensure file server security, you are advised to configure a unique user name for the file server and assign read-only permission to the user to prevent unauthorized modification of the files. After the Auto-Start process is complete, disable the file server function.

3.6.3 Configuring Auto-Start On a Device

This section describes how to configure Auto-Start on a device.

Pre-configuration Tasks

Power on the device and ensure that it completes self-check successfully.

Procedure

Step 1 Configure a management IP address for the device.

1. Run **system-view**

   The system view is displayed.
2. Run **interface** *interface-type interface-number*

   The interface view is displayed.
3. Run **ip address** *ip-address* { *mask* | *mask-length* }

   A management IP address is configured.

   The management IP address is used for device management and maintenance. Configure IP addresses and deploy routes based on network planning to ensure that routes between terminals and devices are reachable.
4. Run **quit**

   Exit from the interface view.

Step 2 Configure file server parameters.

1. Run **autostart**

   The autostart view is displayed.
2. Run **servertype** { **ftp** | **sftp** }

   The type of the file server is configured.

   By default, the file server is an FTP server.
3. Run **ipaddress** *ip*

   The IP address of the file server is configured.
4. Run **username** *username* **password** *password*

 Copyright © Huawei Technologies Co., Ltd.

The user name and password for accessing the file server are configured.

By default, no user is configured for accessing the file server.

5. Run **quit**

   Return to the system view.

6. Run **autostart enable**

   Auto-Start is enabled.

   By default, Auto-Start is disabled on a device.

7. Run **quit**

   Return to the user view.

Step 3 Run **save**

The configuration is saved.

----End

Verifying the Configuration

Run the **display autostart config** command to view configured file server parameters, including the type and IP address of the file server, and the user name and password for accessing the file server.

Follow-up Procedure

After being installed and powered on, the device starts the Auto-Start process.

NOTE

After the Auto-Start process successfully ends, you are advised to run the **undo autostart enable** command to disable Auto-Start and run the **save** command to save the configuration, preventing the device from starting the Auto-Start process again after it restarts the next time.

3.7 Maintaining Auto-Start

You can monitor the running status of Auto-Start in each phase to ensure that Auto-Start runs normally.

- Run the **display autostart status** command to display the running status of Auto-Start.
- Run the **display startup** command to display the system software and configuration files for the current and next startup.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- If the device is connected to the network, you can log in to the device using Telnet or other modes to view the Auto-Start running status, but do not configure the device.
- After downloading a file, do not save the configuration on the device because the configuration has not taken effect. If you save the configuration, the configuration will not take effect after the site deployment process ends.
- You can view the file transfer log on the file server to check whether the device has successfully downloaded the correct system software, patch file, and configuration file.
- If the Auto-Start process is suspended, you can reconfigure file server parameters or the intermediate file and file server, enter the autostart view, and run the **autostart run** command to manually restart the Auto-Start process.

3.8 Configuration Examples for Auto-Start

This section provides Auto-Start configuration examples, including the networking requirements, configuration roadmap, and configuration procedure.

3.8.1 Example for Configuring Auto-Start

Networking Requirements

As shown in **Figure 3-4**, newly-delivered RouterA, RouterB, and RouterC need to be deployed in an enterprise's branches 1, 2, and 3, respectively, and communicate with RouterD in the enterprise's headquarters.

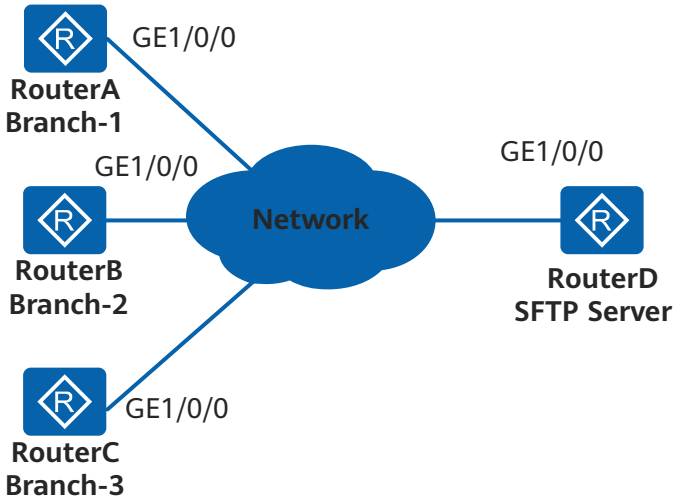
The enterprise wants to load the same system software and different configuration files on RouterA, RouterB, and RouterC. To reduce labor costs for onsite deployment, the enterprise wants to configure these routers remotely and rapidly.

Information of RouterA, RouterB, and RouterC and files to be loaded on these routers are as follows:

- RouterA: The MAC address is 0018-82C5-AA89, ESN is 2102310CXK10B6000183, system software name is V200R007C00.cc, version is V200R007C00, and configuration file is auto_RouterA.cfg.
- RouterB: The MAC address is 0018-82C5-AA90, ESN is 2102310CXK10B6000184, system software name is V200R007C00.cc, version is V200R007C00, and configuration file is auto_RouterB.cfg.
- RouterC: The MAC address is 0018-82C5-AA91, ESN is 2102310CXK10B6000185, system software name is V200R007C00.cc, version is V200R007C00, and configuration file is auto_RouterC.cfg.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-4 Networking for configuring Auto-Start



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure RouterD as the SFTP server.
2. Make the intermediate file **arstart.ini** that maps each router to be configured with the system software and configuration file to be loaded.
3. Save the intermediate file and configuration files and system software to be loaded to the working directory of the SFTP server RouterD, so that RouterA, RouterB, and RouterC can obtain these files.
4. On RouterA, RouterB, and RouterC, configure IP addresses and SFTP server parameters (including the type and IP address of the file server, and the user name and password for accessing the file server), and enable Auto-Start.
5. Power on the routers. The routers use Auto-Start to automatically load configuration files, system software, and patch files.

NOTE

By default, Auto-Start is disabled on a device.

Procedure

Step 1 Configure RouterD as the SFTP server.

Configure the SFTP server function and related parameters.

```
<Huawei> system-view
[Huawei] sysname SFTP Server
[SFTP Server] sftp server enable
[SFTP Server] rsa local-key-pair create
The key name will be: Host
RSA keys defined for Host already exist.
Confirm to replace them? (y/n):y
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is less than 2048,
       It will introduce potential security risks.
```

 Copyright © Huawei Technologies Co., Ltd.

```
Input the bits in the modulus[default = 2048]:2048
Generating keys...
.....................................................................+++
.....................................................+++
.............................+++++++++
.....................+++++++++
```

Configure the user interface for SSH login.

```
[SFTP Server] user-interface vty 0 4
[SFTP Server-ui-vty0-4] authentication-mode aaa
[SFTP Server-ui-vty0-4] protocol inbound all
[SFTP Server-ui-vty0-4] user privilege level 15
[SFTP Server-ui-vty0-4] quit
```

Configure an SSH user.

```
[SFTP Server] aaa
[SFTP Server-aaa] local-user huawei password irreversible-cipher huawei2012
[SFTP Server-aaa] local-user huawei privilege level 15
[SFTP Server-aaa] local-user huawei service-type ssh
[SFTP Server-aaa] local-user huawei ftp-directory sd1:
[SFTP Server-aaa] quit
[SFTP Server] ssh user huawei authentication-type password
```

Configure the IP address of the SFTP server.

```
[SFTP Server] interface gigabitethernet 1/0/0
[SFTP Server-GigabitEthernet1/0/0] ip address 192.168.1.6 255.255.255.0
[SFTP Server-GigabitEthernet1/0/0] quit
```

Step 2 Make the intermediate file **arstart.ini**.

Create a text file and name it **arstart.ini**. The contents and format of the intermediate file are as follows:

```
MAC=0018-82C5-
AA89;ESN=2102310CXK10B6000183;vrpfile=V200R007C00.cc;vrpver=V200R007C00;cfgfile=auto_RouterA.cfg;
MAC=0018-82C5-
AA90;ESN=2102310CXK10B6000184;vrpfile=V200R007C00.cc;vrpver=V200R007C00;cfgfile=auto_RouterB.cfg;
MAC=0018-82C5-
AA91;ESN=2102310CXK10B6000185;vrpfile=V200R007C00.cc;vrpver=V200R007C00;cfgfile=auto_RouterC.cfg;
```

Step 3 Upload the intermediate file, configuration files, and system software to the working directory **sd1** of the SFTP server.

Step 4 Configure IP addresses and SFTP server parameters, and enable Auto-Start on RouterA, RouterB, and RouterC.

Take RouterA as an example. The configurations of RouterB and RouterC are similar to the configuration of RouterA, and are not mentioned here. For details, see the configuration files.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 192.168.1.1 24
[RouterA] autostart
[RouterA-autostart] servertype SFTP
[RouterA-autostart] ipaddress 192.168.1.6
[RouterA-autostart] username huawei password huawei2012
[RouterA-autostart] quit
[RouterA] autostart enable
[RouterA] quit
<RouterA> save
```

Step 5 Start the routers. The routers then start the Auto-Start process.

 Copyright © Huawei Technologies Co., Ltd.

Step 6 Verify the configuration.

After the Auto-Start process ends, log in to routers to be configured and run the **display startup** command to view the startup system software and configuration file. The command output on RouterA is used as an example.

```
<RouterA> display startup
MainBoard:
  Startup system software:                sd1:/V200R007C00.cc
  Next startup system software:           sd1:/V200R007C00.cc
  Backup system software for next startup:  null
  Startup saved-configuration file:       sd1:/auto_RouterA.cfg
  Next startup saved-configuration file:  sd1:/auto_RouterA.cfg
  Startup license file:                   null
  Next startup license file:              null
  Startup patch package:                  null
  Next startup patch package:             null
  Startup voice-files:                    null
  Next startup voice-files:               null
```

Step 7 Disable Auto-Start.

After successfully deploying a router using Auto-Start, disable Auto-Start to prevent the router from starting the Auto-Start process again after it starts the next time. The command output on RouterA is used as an example.

```
<RouterA> system-view
[RouterA] undo autostart enable
[RouterA] quit
<RouterA> save
```

----End

Configuration Files

- RouterD configuration file

```
#
 sysname SFTP Server
#
aaa
 local-user huawei password irreversible-cipher %^%#Wdb-1<0^vO:5yT'Ht^dTY)(+wZ<x>!
GshQKAr7<Lo$fY)(.Y%^%#
 local-user huawei privilege level 15
 local-user huawei ftp-directory sd1:
 local-user huawei service-type ssh
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.6 255.255.255.0
#
 sftp server enable
#
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 15
#
return
```

- RouterA configuration file

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.1 255.255.255.0
#
 autostart enable
autostart
 servertype sftp
```

 Copyright © Huawei Technologies Co., Ltd.

```
 ipaddress 192.168.1.6
 username huawei password %^%#B(Wv8+v`a~b%7c-8L^7G,$)"%^%#
#
return
```

- RouterB configuration file

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.2 255.255.255.0
#
 autostart enable
autostart
 servertype sftp
 ipaddress 192.168.1.6
 username huawei password %^%#B(Wv8+v`a~b%7c-8L^7G,$)"%^%#
#
return
```

- RouterC configuration file

```
#
 sysname RouterC
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.3 255.255.255.0
#
 autostart enable
autostart
 servertype sftp
 ipaddress 192.168.1.6
 username huawei password %^%#B(Wv8+v`a~b%7c-8L^7G,$)"%^%#
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

4 USB-based Deployment Configuration

About This Chapter

USB-based deployment simplifies the deployment process, reduces the deployment costs, and relieves users from software commissioning.

4.1 Overview of USB-based Deployment
This section describes the definition and purpose of USB-based deployment.

4.2 Understanding USB-based Deployment
This section describes the implementation of USB-based deployment.

4.3 Licensing Requirements and Limitations for USB-based Deployment

4.4 Making an Index File
Before USB-based deployment, you must make an index file.

4.5 Performing USB-based Deployment
Before using a USB flash drive to upgrade or configure a device, make an index file, save the index file to the root directory of the USB flash drive, and save files to be loaded to the directory specified in the index file. Then connect the USB flash drive to the device to start the upgrade process. You can use a USB flash drive to upgrade the Android system software versions of the AR161FW-P-M5 running Android versions.

4.6 Configuration Examples for USB-based Deployment
This topic provides a USB-based deployment example. The configuration example includes the networking requirements, configuration roadmap and configuration procedure.

4.1 Overview of USB-based Deployment

This section describes the definition and purpose of USB-based deployment.

Definition

USB-based deployment allows you to configure or upgrade devices using a USB flash drive. Before device deployment, save the deployment files in a USB flash

 Copyright © Huawei Technologies Co., Ltd.

drive. After you connect the USB flash drive to a device, the device downloads the files from the USB flash drive to complete automatic upgrade or service deployment.

Purpose

As the network expands, more and more network devices are used and device deployment becomes more frequent. Traditionally, software engineers have to deploy the devices one by one, which is time-consuming and laborious. USB-based deployment frees software engineers from such trouble. They only need to save the deployment files in a USB flash drive, and then other onsite personnel can finish the deployment process easily. This function simplifies the device deployment process and lowers deployment costs.

Related Documents

Video: **Huawei AR Router USB-based Deployment Feature Introduction**

4.2 Understanding USB-based Deployment

This section describes the implementation of USB-based deployment.

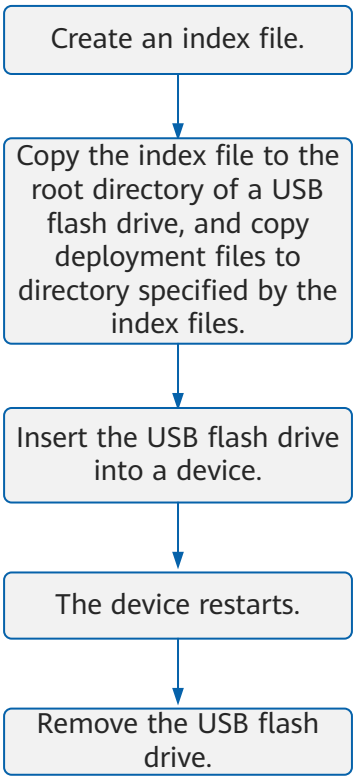
USB-based Deployment Process

Before a USB-based deployment, make an index file, save the index file in the root directory of a USB flash drive, and save the upgrade files in the directory specified in the index file. When you connect the USB flash drive to a device, the device downloads the specified files to complete software upgrade.

Figure 4-1 shows the USB-based deployment flowchart.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-1 USB-based deployment flowchart



Upgrade File Types

The device to be upgraded automatically loads the required files according to description in the index file.

- **Mandatory file**
  - Index file: The file name must be **USB_AR.ini** or **usb_ar.ini**.
- **Optional files**
  - System software: The file name extension is .zip.

    NOTE

    The supported system software format and file name extension vary depending on the AR router model.
  - Configuration file: The file name extension is .cfg, .db, or .zip.
  - Patch file: The file name extension is .pat.
  - License file: The file name extension is .dat.
  - Voice file: The file name extension is .res.
  - Executable file: The file name extension is .sh.

    NOTE

    During USB-based deployment, the standby MPU does not support executable files.
  - User-defined files

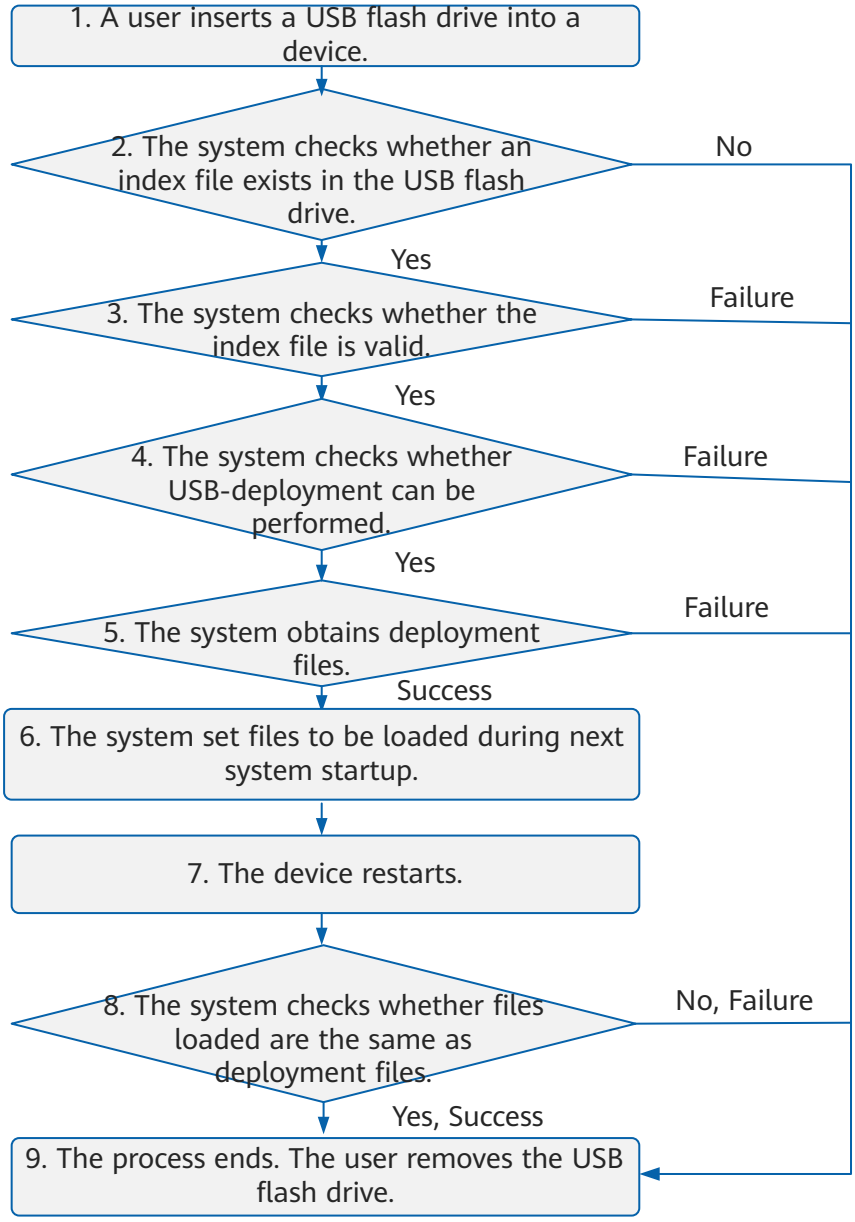
Users can select one or more types of optional file based on the site requirements.

 Copyright © Huawei Technologies Co., Ltd.

Device Running Process

Figure 4-2 shows the device running flowchart during USB-based deployment.

Figure 4-2 Device running flowchart



1. A user inserts a USB flash drive to a device.
2. The system detects the USB flash drive and checks whether an index file exists in the USB flash drive.
   - If an index file exists, the process goes to step 3.
   - If no index file exists, the USB-based deployment process ends.
3. The system checks whether the index file is valid.
   - If the index file is valid, the process goes to step 4.

 Copyright © Huawei Technologies Co., Ltd.

   - If the index file is invalid, the deployment fails.
4. The system checks whether USB-based deployment can be performed.
   - If USB-based deployment can be performed, the process goes to step 5.
   - If USB-based deployment cannot be performed, the deployment fails.

   NOTE

   When the current configuration file of the device is not empty, the USB-based deployment function must be enabled using the **autoupdate enable** command in the deployment configuration file and the password used for USB-based deployment must be configured. Otherwise, the device cannot be configured using the USB flash drive.
5. The system obtains deployment files from the USB flash drive and saves them in specified storage media.
   - If files are obtained successfully, the process goes to step 6.
   - If files are not obtained successfully, the deployment fails.

   NOTE

   If the system software package fails verification during USB-based deployment, the upgrade process will not be terminated immediately. Instead, the system continues to verify other types of files and loads these files for the upgrade if the files pass verification.
6. The system specifies the loaded files for next startup.
7. The device restarts.
8. The system checks whether the loaded files are the same as the specified upgrade files.
   - If so, the deployment succeeds.
   - If not, the deployment fails.
9. The USB-based deployment process ends. The user removes the USB flash drive from the device.

USB-based Android Operating System Upgrade

You can upgrade the Android operating system versions of AR161-FW-P-M5 using a USB flash drive. Before a USB-based upgrade, save the Android operating system version **update.zip** and configuration file **once.cfg** or **unlmt.cfg** in the **dload** folder in the root directory of a USB flash drive.

once.cfg and **unlmt.cfg** are two empty text documents, indicating one-time upgrade and unlimited upgrade. The two files cannot co-exist. After an upgrade begins, the green indicator blinks every 1 second. If the upgrade fails, the device restarts after the red indicator remains steady on for 30 seconds.

- One-time upgrade: After a USB flash drive is inserted in a device, the device compares the sizes (accurate to bytes) of two **update.zip** files: one in use and the other in the USB flash drive. If the two files have different sizes, the device begins to upgrade. If the upgrade succeeds, the device restarts after the green indicator remains steady on for 3 seconds. After the device restarts, the device runs the **update.zip** file copied from the USB flash drive. In this situation, the size of the **update.zip** file currently used by the device is the same as that in the USB flash drive, and the restarted device is not upgraded again.
- Unlimited upgrade: After a USB flash drive is inserted in a device, the device restarts and upgrades without comparing the sizes of two **update.zip** files:

 Copyright © Huawei Technologies Co., Ltd.

one in use and the other in the USB flash drive. After an unlimited upgrade succeeds, the device does not restart or continues to upgrade. After the USB flash drive is removed from the device, the device restarts to complete the upgrade.

NOTE

Removing a USB flash drive from a device during an upgrade may cause the device unable to start. You can insert the USB flash drive in the device again to rectify this fault.

On the AR161FW-P-M5 only the OSP daughter card supports the Android operating system. Therefore, you can check whether the OSP daughter card is upgraded successfully only through the connected screen because the USB-based deployment indicator cannot show whether the OSP daughter card is upgraded successfully.

4.3 Licensing Requirements and Limitations for USB-based Deployment

Involved Network Elements

None

Licensing Requirements

USB-based deployment is a basic feature of a router and is not under license control.

Feature Limitations

- Currently, streamlined USB-based deployment can only be used in the SD-WAN Solution. Devices with dual SRUs do not support this deployment mode.
- When using an interface on an LPU for streamlined USB-based deployment, insert a USB flash drive for deployment after the LPU is registered successfully. Otherwise, you need to restart the device and then deploy it. During the deployment, determine the LPU registration status and deployment status based on the indicator status.
- After the deployment is complete, ensure that the devices are deployed based on the mapping between ESNs and sites. Otherwise, the network between the devices and controller may be unreachable.
- During USB-based deployment, if there is system software in deployment files, the CPU usage may become high temporarily. The CPU usage will automatically return to the normal range, without requiring any action.
- When creating a VM through USB-based deployment on the AR169-P-M9, AR169W-P-M9, or AR169RW-P-M9, ensure that the size of the VM installation package **.ova** is less than 50 GB. Otherwise, the USB-based deployment will fail.

4.4 Making an Index File

Before USB-based deployment, you must make an index file.

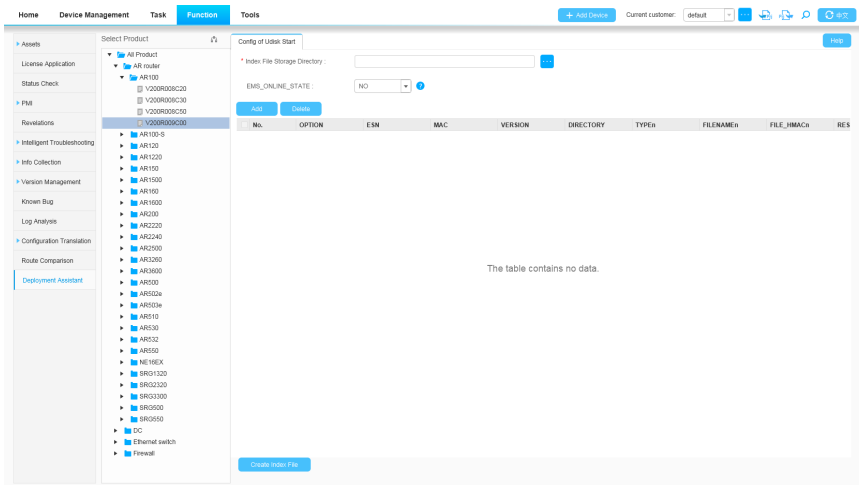
 Copyright © Huawei Technologies Co., Ltd.

Procedure of Making an Index File

Two methods are available to make an index file of USB-based deployment: use a text file to edit the index file or use eDesk to make an index file.

- Method 1: Edit the index file on the PC:
  a. Create a text file.
  b. Edit the file based on the index file format.
  c. Rename the file as **USB_AR.ini**.
  d. Copy the **USB_AR.ini** file to the root directory of the USB flash drive.
- Method 2: Use eDesk to make an index file:
  a. Log in to eDesk.
  b. Choose **Function** > **Deployment Assistant**. In **Select Product**, select the corresponding product to access the **Config of Udisk Start** page, as shown in **Figure 4-3**.

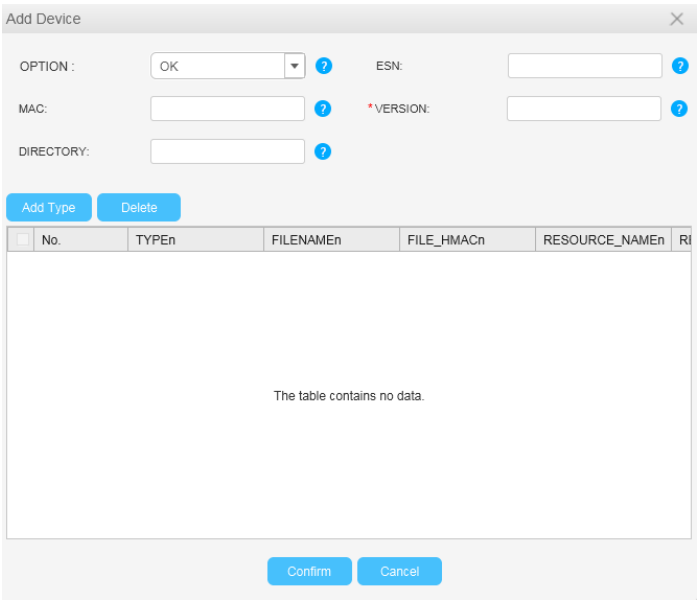
Figure 4-3 Config of Udisk Start



  c. On the **Config of Udisk Start** page, click **Add** to access the **Add Device** page, as shown in **Figure 4-4**. Set related parameters. For details, see **Table 4-1**.

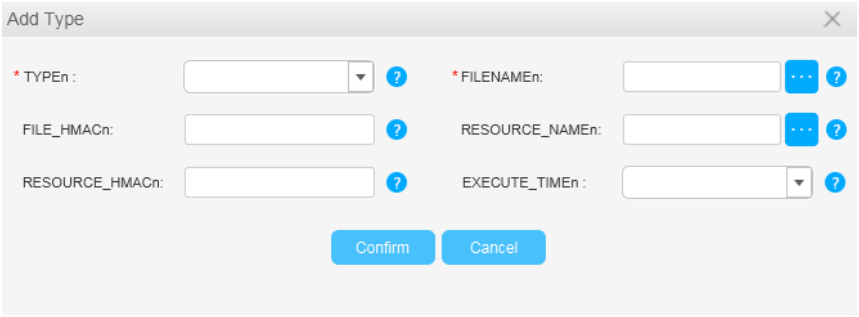
 Copyright © Huawei Technologies Co., Ltd.

Figure 4-4 Add Device



d. On the **Add Device** page, click **Add Type**. In the displayed dialog box **Add Type**, select the file type, as shown in **Figure 4-5**.

Figure 4-5 Add Type

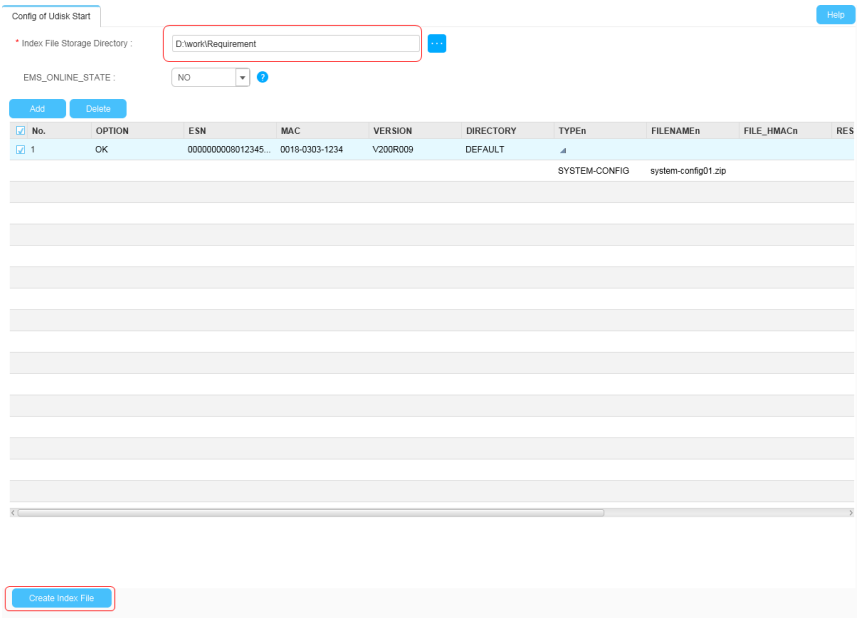


In the dialog box **Add Type**, set parameters and click **Confirm** to save the file type. Return to the **Add Device** page, and click **Confirm** to save device information.

e. On the **Config of Udisk Start** page, specify a directory for **Index File Storage Directory**, select the created index data, and click **Create Index File**, as shown in **Figure 4-6**.

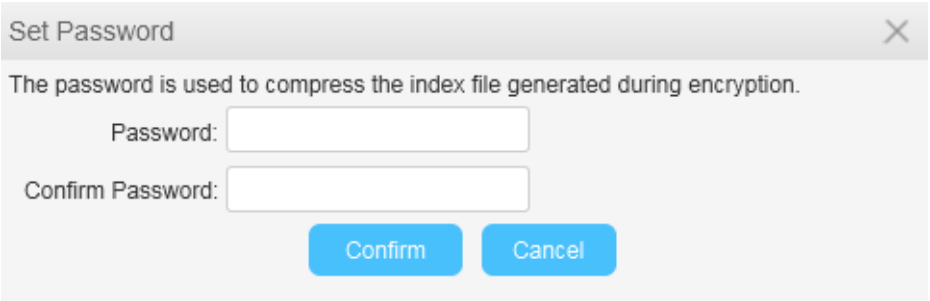
 Copyright © Huawei Technologies Co., Ltd.

Figure 4-6 Create Index File



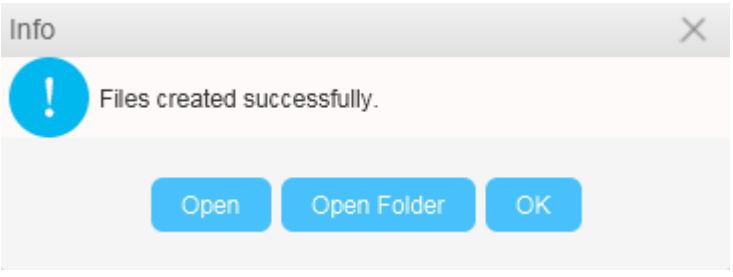
f. In the displayed dialog box, set the password used to generate an index file, as shown in **Figure 4-7**, and then click **Confirm**.

Figure 4-7 Set Password



g. You have created an index file successfully, as shown in **Figure 4-8**.

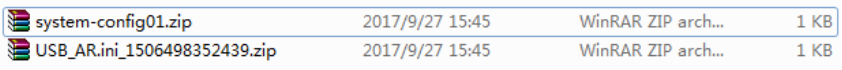
Figure 4-8 Creating an index file successfully



 Copyright © Huawei Technologies Co., Ltd.

h. In the displayed dialog box, click **Open Folder** to access the index file storage directory and obtain the corresponding index file, as shown in Figure 4-9. The **USB_AR.ini** in the **USB_AR.ini_1506498352439.zip** indicates the generated index file.

Figure 4-9 Index file



Index File Format

The index file format is as follows:

```
BEGIN AR
[USB CONFIG]
SN=
EMS_ONLINE_STATE=
[UPGRADE INFO]
OPTION=
DEVICENUM=
[DEVICEn DESCRIPTION]
OPTION=
ESN=
MAC=
VERSION=
DIRECTORY=
FILENUM=
TYPEn=
FILENAMEn=
FILE_HMACn=
RESOURCE_NAMEn=
RESOURCE_HMACn=
EXECUTE_TIMEn=
END AR
```

Table 4-1 Fields in the index file

Field	Description
BEGIN AR	Start tag of the index file. This field cannot be modified. This field is mandatory.
USB CONFIG	USB flash drive configuration. This field cannot be modified. This field is mandatory.

 Copyright © Huawei Technologies Co., Ltd.

Field	Description
SN	Data change time in the format *YearMonthDay*.*HourMinuteSecond*. For example, the value **20110628.080910** indicates 2011-06-28 08:09:10. This field is mandatory. **NOTE** The SN field is a USB-based deployment flag. A device has a default USB-based deployment flag. If the **USB_AR.ini** file exists in the USB flash drive, the device checks whether the default USB-based deployment flag and the SN value in the **USB_AR.ini** file are the same. If they are different, the USB-based deployment process is triggered. If the deployment succeeds, the value of the default USB-based deployment flag on the device is changed to the SN value in the **USB_AR.ini** file.
EMS_ONLINE_STATE	Whether the NMS is online: ● **YES**: The NMS is online. ● **NO**: The NMS is offline. This field is mandatory.
UPGRADE INFO	Upgrade information header. This field cannot be modified. This field is mandatory.
OPTION	Upgrade mode flag. The field has a fixed value of **AUTO**. This field is mandatory.
DEVICENUM	Number of devices to be upgraded using this index file. The value is an integer that ranges from 1 to 100. ● To upgrade the software version of one device, set the value of the DEVICENUM field to **1** and use the device's ESN and MAC address. ● To upgrade software versions of multiple devices of the same series to the same version, set the value of the DEVICENUM field to **1** and use the default ESN and MAC address. ● To upgrade software versions of multiple devices of the same series to different versions, set the value of the DEVICENUM field to the number of devices to be upgraded and use devices' ESNs and MAC addresses. This field is mandatory.

 Copyright © Huawei Technologies Co., Ltd.

Field	Description
DEVICE*n* DESCRIPTION	Description information header of device *n*. The value of *n* is an integer that ranges from 1 to 100. This field is mandatory. **NOTE** The value *n* must be set when you make the index file.
OPTION	Whether USB-based deployment is required for the device. The value **OK** indicates that USB-based deployment is required, and the value **NOK** indicates that USB-based deployment is not required. This field is mandatory.
ESN	Serial number of a device. If the value of this field is **DEFAULT**, the index file is applicable to all devices. Otherwise, the index file is applicable to a specific device. This field is mandatory. **NOTE** If this field is left empty, this field matches all devices.
MAC	MAC address of a device. If the value of this field is **DEFAULT**, the index file is applicable to all devices. Otherwise, the index file is applicable to a specific device. This field is mandatory. **NOTE** If this field is left empty, this field matches all devices.
VERSION	Version number after the upgrade. This field is mandatory. **NOTE** The version must be entered correctly. Otherwise, the device will fail to be upgraded.
DIRECTORY	Path for storing deployment files. ● If the value is **DEFAULT**, the deployment files are stored in the root directory of the USB flash drive. ● If the value is **/abc**, the deployment files are stored in the **abc** directory. This field is mandatory. **NOTE** If this field is left empty, the deployment files are saved in the root directory of the USB flash drive.

 Copyright © Huawei Technologies Co., Ltd.

Field	Description
FILENUM	Number of files to be loaded. If only the system software needs to be loaded, the value of this field is set to **1**. If the system software and patch file need to be loaded, the value of this field is set to **2**. This field is mandatory.

Field	Description
TYPE*n*	Upgrade file type: • **FACTORY-CONFIG**: factory configuration file. **NOTE** If the device supports the voice function and works as a PBX, the configuration file is **FACTORY-CONFIG-PBX**. If the device supports the voice function and works as an AG, the configuration file is **FACTORY-CONFIG-AG**. • **SYSTEM-SOFTWARE**: system software. • **SYSTEM-OSP**: VM installation package in OVA format. • **SYSTEM-CONFIG**: configuration file. **NOTE** If the device supports the voice function and works as a PBX, the configuration file is **SYSTEM-CONFIG-PBX**. If the device supports the voice function and works as an AG, the configuration file is **SYSTEM-CONFIG-AG**. • **SYSTEM-PAT**: patch file. • **SYSTEM-LICENSE**: license file. **NOTE** If license files need to be loaded in a batch, the device provides the function of automatically matching license file names without requiring license file names to be manually modified, improving batch deployment efficiency. If license files need to be loaded in a batch using the USB-based deployment function, the FILENAMEn field for SYSTEM-LICENSE in the index file must be set to DEFAULT. • **SYSTEM-VOICE**: voice file. • **SYSTEM-EXECUTE**: executable file, which can be only the shell type. • **USER-DEFINE**: user-defined file.

 Copyright © Huawei Technologies Co., Ltd.

Field	Description
	NOTE The AR169-P-M9, AR169W-P-M9, and AR169RW-P-M9 support USB-based VM creation. The requirements are as follows: • If the device does not contain a configuration file, the parameters in the index file **USB_AR.ini** for USB-based deployment are set as follows: **TYPE***n1* is set to **SYSTEM-OSP**, **FILENAME***n1* to *VM installation package.ova*, **TYPE***n2* to **SYSTEM-CONFIG**, and **FILENAME***n2* to **osp_cfg.cfg**. The content format of the **osp_cfg.cfg** file is "*vm-name*;*port-num*;*password*;", for example, **vm2;3;Admin123;**. • *vm-name*: specifies the VM name. The value is a string of 1 to 32 case-sensitive characters and consists of letters and digits. • *port-num*: specifies the VNC service port number. The value is an integer that ranges from 1 to 8. • *password*: specifies the password for VNC authentication. The value is a string of 6 to 8 case-sensitive characters without spaces. • If the device contains a configuration file, the parameters in the index file **USB_AR.ini** for USB-based deployment are set as follows: **TYPE***n1* is set to **SYSTEM-OSP**, **FILENAME***n1* to *VM installation package.ova*, **TYPE***n2* to **SYSTEM-CONFIG**, and **FILENAME***n2* to **osp_cfg.zip**. The **osp_cfg.zip** file is encrypted and compressed from the **osp_cfg.cfg** file. The value of *n* is an integer that starts from 1. This field is mandatory.
FILENAME*n*	Upgrade file name. For example, if the value of the TYPE1 field is **SYSTEM-EXECUTE** and the name of the executable file corresponding to the U disk is **test_execute.sh**, the value of the FILENAME1 field is **test_execute.sh**. The value of *n* is an integer that starts from 1. This field is mandatory.
FILE_HMAC*n*	HMAC used to verify a file to be downloaded. The MAC address is a string of 64 characters that is calculated for a specific file using a file checker based on the HMAC-SHA256 algorithm. The key used to calculate the HMAC must be the same as the password configured by the **set usb autoupdate password** command. The value of *n* is an integer that starts from 1. **NOTE** This field is optional. This field is mandatory after the **hmac enable** command is executed to enable HMAC check for USB-based deployment.

 Copyright © Huawei Technologies Co., Ltd.

Field	Description
RESOURCE_NAME*n*	Name of the resource file to be upgraded. You can perform operations on the resource file through an executable file. For example, copy the resource file to the device. The resource file must be saved in the root directory of the USB flash drive. The value of *n* is an integer that starts from 1. This field is optional.
RESOURCE_HMAC*n*	Information used to perform HMAC check on the loaded resource file. The MAC address is a string of 64 characters that is calculated for a specific file using a file checker based on the HMAC-SHA256 algorithm. The key used to calculate the HMAC must be the same as the password configured by the **set usb autoupdate password** command. The value of *n* is an integer that starts from 1. **NOTE** This field is optional. This field is mandatory after the **hmac enable** command is executed to enable HMAC check for USB-based deployment.
EXECUTE_TIME*n*	Execution time of an executable file: ● 0: Before the deployment ● 1: After the deployment The value of *n* is an integer that starts from 1. This field is optional. This field is mandatory when upgrade files contain an executable file.
END AR	End tag of the index file. This field is mandatory.

Examples

Example 1

You need to create an index file for upgrading one device, and the requirements are as follows:

- Data is changed at 08:09:10 on June 28, 2013.
- The NMS is offline.
- Upgrade is required.
- The device ESN is 00080123456789 and the MAC address is 0018-0303-1234.
- The system software **system-software01.cc** is stored in the root directory of the USB flash drive. The version number is V200R010. The HMAC string is c3caaee8f4f6bd1389f438801e40dad9af30f2fbbe7e8f55121b39c6c16ba488.

The index file that meets the preceding requirements is as follows:

 Copyright © Huawei Technologies Co., Ltd.

```
BEGIN AR
[USB CONFIG]
SN=20130628.080910
EMS_ONLINE_STATE=NO
[UPGRADE INFO]
OPTION=AUTO
DEVICENUM=1
[DEVICE1 DESCRIPTION]
OPTION=OK
ESN=00080123456789
MAC=0018-0303-1234
VERSION=V200R010
DIRECTORY=DEFAULT
FILENUM=1
TYPE1=SYSTEM-SOFTWARE
FILENAME1=system-software01.cc
FILE_HMAC1=c3caaee8f4f6bd1389f438801e40dad9af30f2fbbe7e8f55121b39c6c16ba488
END AR
```

Example 2

You need to create an index file for upgrading multiple devices of the same series to the same software version, and the requirements are as follows:

- Data is changed at 08:09:10 on June 28, 2013.
- The NMS is offline.
- Upgrade is required.
- The system software **system-software01.cc** is stored in the root directory of the USB flash drive. The version number is V200R010. HMAC check is not required for any file.

The index file that meets the preceding requirements is as follows:

```
BEGIN AR
[USB CONFIG]
SN=20130628.080910
EMS_ONLINE_STATE=NO
[UPGRADE INFO]
OPTION=AUTO
DEVICENUM=1
[DEVICE1 DESCRIPTION]
OPTION=OK
ESN=DEFAULT
MAC=DEFAULT
VERSION=V200R010
DIRECTORY=DEFAULT
FILENUM=1
TYPE1=SYSTEM-SOFTWARE
FILENAME1=system-software01.cc
END AR
```

Example 3

You need to create an index file for two devices with different description information, and the requirements are as follows:

- Data is changed at 08:09:10 on June 28, 2013.
- The NMS is offline.
- The ESN of the first device is 00080123456789. The MAC address is 0018-0303-1234. The name of the system software is **V200R010.cc**. The version number is V200R010. The configuration file **system-config01.zip** must be loaded. HMAC check is not required for any file.

 Copyright © Huawei Technologies Co., Ltd.

- The ESN of the second device is 66680123456789. The MAC address is 0018-0303-5678. The name of the system software is **V200R010.cc**. The version number is V200R010. The configuration file **system-config02.zip** must be loaded. HMAC check is not required for any file.

The index file that meets the preceding requirements is as follows:

```
BEGIN AR
[USB CONFIG]
SN=20130628.080910
EMS_ONLINE_STATE=NO
[UPGRADE INFO]
OPTION=AUTO
DEVICENUM=2
[DEVICE1 DESCRIPTION]
OPTION=OK
ESN=00080123456789
MAC=0018-0303-1234
VERSION=V200R010
DIRECTORY=DEFAULT
FILENUM=2
TYPE1=SYSTEM-SOFTWARE
FILENAME1=V200R010.cc
TYPE2=SYSTEM-CONFIG
FILENAME2=system-config01.zip
[DEVICE2 DESCRIPTION]
OPTION=OK
ESN=66680123456789
MAC=0018-0303-5678
VERSION=V200R010
DIRECTORY=DEFAULT
FILENUM=2
TYPE1=SYSTEM-SOFTWARE
FILENAME1=V200R010.cc
TYPE2=SYSTEM-CONFIG
FILENAME2=system-config02.zip
END AR
```

Example 4

You need to create an index file for VM installation, and the requirements are as follows:

- Data is changed at 08:09:10 on January 7, 2016.
- The NMS is offline.
- VM installation is required.
- The VM installation package (OVA file) **usb.ova** is stored in the root directory of the USB flash drive. The version number is V200R007C00. The HMAC string is 5c27a53005048beaa9f518da42912484edbf6bdd5a157ea777c8e80087a08b03.
- The VM configuration file **osp_cfg.zip** is stored in the root directory of the USB flash drive. The HMAC string is a1735904e3df0abf0bc2a3a7a32f33ecd641eaeb575ba4f5e88810df92c7fdce.

The index file that meets the preceding requirements is as follows:

```
BEGIN AR
[USB CONFIG]
SN=20160107.080910
EMS_ONLINE_STATE=NO
[UPGRADE INFO]
OPTION=AUTO
DEVICENUM=1
[DEVICE1 DESCRIPTION]
```

 Copyright © Huawei Technologies Co., Ltd.

```
OPTION=OK
ESN=DEFAULT
MAC=DEFAULT
VERSION=V200R007C00
DIRECTORY=DEFAULT
FILENUM=2
TYPE1=SYSTEM-OSP
FILENAME1=usb.ova
FILE_HMAC1=5c27a53005048beaa9f518da42912484edbf6bdd5a157ea777c8e80087a08b03
TYPE2=SYSTEM-CONFIG
FILENAME2=osp_cfg.zip
FILE_HMAC2=a1735904e3df0abf0bc2a3a7a32f33ecd641eaeb575ba4f5e88810df92c7fdce
END AR
```

Example 5

You need to create an index file to upgrade the configuration file, Android package (APK) file, Android database file, and Android boot logo file, and the requirements are as follows:

- Data is changed at 08:09:10 on August 25, 2016.
- The NMS is offline.
- Upgrade is required.
- The configuration file is stored in the root directory of the USB flash drive and named **vrpcfg.cfg**.
- The master Android system database file is stored in the root directory of the USB flash drive and named **settings.db**.
- The slave Android system database file is stored in the root directory of the USB flash drive and named **mos_settings.db**.
- The APK file is stored in the root directory of the USB flash drive and named **Player.apk**.
- The Android boot logo file is stored in the root directory of the USB flash drive and named **bootanimation_armaster.zip**.

To install the APK file, Android database file, and Android boot logo file during USB-based deployment, you must use executable files and an app detection file. Executable files are stored in the root directory of the USB flash drive and named **huawei_execute1.sh**, **huawei_execute2.sh**, and **huawei_execute3.sh**, and an app detection file is stored in the root directory of the USB flash drive and named **app-list.xml**.

The index file that meets the preceding requirements is as follows:

```
BEGIN AR
[USB CONFIG]
SN=20160825.080910    //The SN needs to be changed during each device deployment. The current time is recommended as the SN.
EMS_ONLINE_STATE=NO
[UPGRADE INFO]
OPTION=AUTO
DEVICENUM=1    //Number of devices to be upgraded.
[DEVICE1 DESCRIPTION]
OPTION=OK
ESN=DEFAULT
MAC=DEFAULT
VERSION=V200R006C12    //Upgrade version. It must be correct; otherwise, the deployment will fail.
DIRECTORY=DEFAULT
FILENUM=6    //Actual number of deployment files.
TYPE1=SYSTEM-EXECUTE    //The app-list.xml file is mandatory.
FILENAME1=huawei_execute1.sh
```

 Copyright © Huawei Technologies Co., Ltd.

```
RESOURCE_NAME1=app-list.xml
EXECUTE_TIME1=0
TYPE2=SYSTEM-EXECUTE    //Executable files can be increased based on the number of deployment apps.
FILENAME2=huawei_execute2.sh
RESOURCE_NAME2=Player.apk
EXECUTE_TIME2=0
TYPE3=SYSTEM-CONFIG    //VRP configuration file.
FILENAME3=vrpcfg.cfg
TYPE4=SYSTEM-CONFIG    //Master Android system database file.
FILENAME4=settings.db
TYPE5=SYSTEM-CONFIG    //Slave Android system database file.
FILENAME5=mos_settings.db
TYPE6=SYSTEM-EXECUTE       //Boot logo file.
FILENAME6=huawei_execute3.sh
RESOURCE_NAME6=bootanimation_armaster.zip
EXECUTE_TIME6=0
END AR
```

Edit executable files.

New folders can be created and APK files can be copied on a device after the device reads the **SYSTEM-EXECUTE** field and executes the **huawei_execute1.sh** file. The **huawei_execute1.sh** file is as follows:

```
#!/bin/sh
mkdir -p /mnt/rom/usbresource
cp -r $1 /mnt/rom/usbresource
chmod 777 -R /mnt/rom/usbresource
```

Subsequent executable files (**huawei_execute2.sh** and **huawei_execute3.sh**) have the same content and must be named differently depending on APK files so that APK files can be automatically copied from the USB flash drive to a device. The content is as follows:

```
#!/bin/sh
cp -r $1 /mnt/rom/usbresource
chmod 777 -R /mnt/rom/usbresourcee
```

Editing the app detection file app-list.xml.

The format of an app detection file is as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<list>
<apk>
<name>com.huawei.subpackagename</name>
<version>20141024</version>
<target>ARMaster</target>
<status>install</status>
<startinfo>com.huawei.subpackagename,com.huawei.subpackagename.MainActivity</startinfo>
<url>/mnt/vrprootfs/mnt/rom/usbresource/player.apk</url>
</apk>
<apk>
<name>com.huawei.subpackagename</name>
<version>20141024</version>
<target>ARSlave</target>
<status>uninstall</status>
<startinfo>com.huawei.subpackagename,com.huawei.subpackagename.MainActivity</startinfo>
<url>/mnt/vrprootfs/mnt/rom/usbresource/player.apk</url>
</apk>
</list>
```

 Copyright © Huawei Technologies Co., Ltd.

Table 4-2 Fields in an app detection file

Field	Description
<list></list>	The app detection file is in list format.
<apk></apk>	APK information to be configured. **NOTE** If the device needs to operate multiple APK files, add multiple such fields to the app detection file.
<name></name>	Name of the APK software package.
<version></version>	APK version number. **NOTE** The value of this field must be the same as the version of the APK file to be installed, uninstalled, or updated; otherwise, the device repeatedly installs, uninstalls, or updates the APK file.
<target></target>	Android system type of the APK file: ● ARMaster: indicates the master Android system. ● ARSlave: indicates the slave Android system.
<status></status>	Operation type: ● install: installs an APK file. ● uninstall: uninstalls an APK file.
<startinfo></startinfo>	Automatic APK startup information, in the format "<startinfo>package name, path and type of the main Activity to be started<startinfo>". If an APK file has the automatic startup attribute and is expected to start after the device starts, this field must be configured.
<url></url>	Storage path of an APK file on the device.

4.5 Performing USB-based Deployment

Before using a USB flash drive to upgrade or configure a device, make an index file, save the index file to the root directory of the USB flash drive, and save files to be loaded to the directory specified in the index file. Then connect the USB flash drive to the device to start the upgrade process. You can use a USB flash drive to upgrade the Android system software versions of the AR161FW-P-M5 running Android versions.

Background

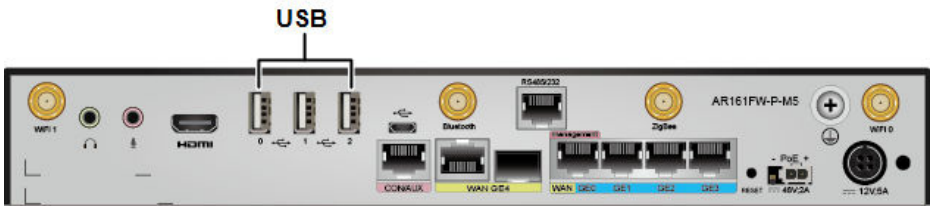
The USB-based deployment process varies according to the deployment file type and whether the device has the configuration.

 Copyright © Huawei Technologies Co., Ltd.

File Type	Unconfigured Device	Configured Device
Configuration file (including the Android configuration file)	Connect the USB flash drive to the device to start the USB-based deployment process. The Android configuration file supports the database file format (with a fixed file name **settings.db**) and password-free ZIP file format (with any file name).	Enable the USB-based deployment function on the device before connecting the USB flash drive to it. Otherwise, the device cannot be configured using the USB flash drive. The Android configuration file supports only the ZIP file format with any file name. The file **settings.db** (with a fixed file name) is encrypted and compressed into a .zip file, and the encryption password is the same as the authentication password for USB-based deployment.
Non-configuration file (system software and patches)	Connect the USB flash drive to the device to start the USB-based deployment process.	• Connect the USB flash drive to the device to start the USB-based deployment process without any check. • Enable the USB-based deployment function on the device before connecting the USB flash drive to it.

On the AR161FW-P-M5 running an Android version, the OSP daughter card has different system software than the device. You can only save the Android system software (with the file name fixed as **update.zip**) and configuration file (**once.cfg** or **unlmt.cfg**) to the **dload** folder in the root directory of a USB flash drive to directly upgrade the Android system software version of the OSP daughter card. The USB flash drive can only be connected to the USB port of the OSP daughter card, as shown in **Figure 4-10**. You can only make an index file **USB_AR.ini** to upgrade the system software of the AR161FW-P-M5. The USB flash drive needs to be connected to the USB port of the device, as shown in **Figure 4-11**.

Figure 4-10 USB port on the AR161FW-P-M5 OSP daughter card



 Copyright © Huawei Technologies Co., Ltd.

Figure 4-11 USB port on the AR161FW-P-M5



Pay attention to the following points during a USB-based deployment:

- The USB flash drive must support the FAT32 file system and its interface must be a standard USB 2.0 or USB 3.0 interface.

  NOTE

  - If the file system format of the USB flash drive is not FAT32, convert the format into FAT32 (format the USB flash drive) before using the USB flash drive.
  - The AR169W-P-M9, AR169RW-P-M9 support USB-based VM creation. If the size of the VM installation package (OVA file) is greater than 4 GB, the file system format of the USB flash drive must be ext4 (or you can convert the format into ext4).
  - The USB3.0 interface is running on the AR169CVW-4B4S, AR161EW, AR161EW-M1, AR169EW, AR169EGW-L, AR169CVW.
  - You are advised to use a USB flash drive whose storage size is less than 64 GB.
- USB flash drives from different vendors differ in model compatibility and drivers. If a USB flash drive cannot be used, try to replace it with another one from a mainstream vendor.
- Before saving files to a USB flash drive, disable the write-protection function of the USB flash drive.
- Before performing a USB-based deployment, ensure that the device is working properly and its flash memory or SD card has sufficient space for files to be loaded.
- The device can start using system software in the USB flash drive. When the device cannot start, for example, the storage medium is formatted, power off the device, install the USB flash drive with system software on the device, and then power on the device.
- Only a USB flash drive with one or no partition can be installed on the device. A USB flash drive with multiple partitions cannot be installed.
- Before installing a USB flash drive on the device, ensure that the USB flash drive has been formatted and file systems have been created. The device does not support a USB flash drive without file systems.
- Only one USB flash drive can be connected to a device.

 Copyright © Huawei Technologies Co., Ltd.

- Files used for USB-based deployment include index file, system software, configuration file, patch file, voice file, license file, executable file, and User-defined files. The index file is mandatory. Among the other files, at least one must be saved in the USB flash drive.
- Do not power off the device when the device is copying files. Otherwise, the upgrade fails or the device cannot start.
- Do not remove the USB flash drive before the upgrade is finished. Otherwise, data in the USB flash drive may be damaged.

Pre-configuration Tasks

Before performing a USB-based deployment, power on the device and ensure that the device runs normally.

Procedure

1. Make an index file.

   For details on how to make an index file, see **4.4 Making an Index File**.
2. Save the index file and the resource file to be loaded to the device to the root directory of the USB flash drive and save the files specified in the index file to the specified directory.

   The DIRECTORY field to the index file specifies the directory for files to be loaded:

   – If DIRECTORY is set to DEFAULT, save the files to the root directory of the USB flash drive.

   – If DIRECTORY is set to /abc, save the files to the **abc** directory.
3. Enable the USB-based deployment function on the device. Skip this step if the device has no configuration. If the device is deployed using non-configuration files, you can skip this step.

   a. Run the **set usb autoupdate password** *password* command in the system view to configure an authentication password for USB-based deployment.

      The password configured using the **set usb autoupdate password** command must contain at least two types of characters, uppercase and lowercase characters, digits, and special characters excluding spaces and question marks (?).

      The authentication password configured by this command is used in the following scenarios:

      - When hash-based message authentication code (HMAC) check is enabled, the device uses this password as the key to calculate the HMAC.

        NOTE

        Currently, the HMAC can only be calculated using the HMAC-SHA256 algorithm.

      - When downloading an encrypted configuration file from the USB flash drive, the device uses this password to decrypt the configuration file.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Currently, configuration files can be encrypted only when they are being compressed into a .zip format. The following encryption methods can be used:

- Simple text encryption: For example, when you compress a .cfg configuration file into a .zip file, you can enter a password in the compression software to encrypt the configuration file.
- AES256 encryption algorithm: For example, when you compress a .cfg configuration file into a .zip file, you can select the AES256 mode and enter a password in the compression software to encrypt the configuration file. This encryption method is recommended because it is more secure.

It is recommended that you encrypt the configuration file to enhance security. The password used to encrypt the configuration file must be the same as the password configured by the **set usb autoupdate password** command.

b. (Optional) Run the **hmac enable** command in the system view to enable HMAC check for USB-based deployment.

After HMAC check is configured for USB-based deployment, the device uses the password configured by the **set usb autoupdate password** command as the key to calculate an HMAC based on the HMAC-SHA256 algorithm for a specific file. Then the device compares the calculated HMAC with the value of the HMAC field in the index file. If the two HMAC values are the same, the device considers the file to be downloaded valid.

NOTE

After HMAC check is configured for USB-based deployment, the device performs HMAC check for all the files used for startup. If this function is not enabled, the device does not perform HMAC check when downloading files from the USB flash drive.

If HMAC check is enabled, the HMAC field in the index file must contain the HMAC.

It is recommended that you enable HMAC check for USB-based deployment to enhance security.

c. (Optional) Run the **usb autoupdate generate encrypted boot-password** command in the system view to encrypt a Boot password in plain text into one in cipher text.

d. Run the **autoupdate enable** command in the system view to enable the USB-based deployment function.

NOTE

This command can take effect only after an authentication password for USB-based deployment is configured by the **set usb autoupdate password** command.

4. Connect the USB flash drive to the device to start the USB-based deployment process.

During the deployment, the system obtains the required files according to content in the index file (**USB_AR.ini**) and saves the files in the default storage medium. Then the device specifies the new system software and configuration file as the files for next startup, and restarts.

 Copyright © Huawei Technologies Co., Ltd.

Procedure for Using a USB Flash Drive to Upgrade the Android System Software

1. Make the configuration file.

   Create a text file and name it **once.cfg** or **unlmt.cfg** according to requirements. For details, see **4.2 Understanding USB-based Deployment**.
2. Create the **dload** folder in the root directory of the USB flash drive and save the Android system software **update.zip** and made configuration file to the root directory.
3. Connect the USB flash drive to the device to start the upgrade process.
   - To upgrade the Android system software of the AR161FW-P-M5, you can only connect the USB flash drive to the USB port of the OSP daughter card, as shown in **Figure 4-10**.

NOTE

Removing the USB flash drive during an upgrade may cause the device unable to start. You can install the USB flash drive again to solve the problem.

After the upgrade succeeds, you can use the USB flash drive to roll back to the previous Android system software version.

Verifying the Configuration

- Run the **display usb** *usb-id* **autoupdate state** command to check the progress of USB-based deployment.
- Observe the USB indicator on the device to determine the progress of USB-based deployment:
  - Steady green: The USB-based deployment succeeded.
  - Blinking green: The system USB-based deployment is ongoing.
  - Steady red: USB-based deployment has failed.

NOTE

After the USB-based deployment succeeds, remove the USB flash drive from the device.

4.6 Configuration Examples for USB-based Deployment

This topic provides a USB-based deployment example. The configuration example includes the networking requirements, configuration roadmap and configuration procedure.

4.6.1 Example for Configuring USB-based Deployment

Networking Requirements

Two devices need to be automatically upgraded, and no software engineers are available onsite. The requirements are as follows:

- The devices need to be upgraded at 08:09:10 a.m. on October 8, 2014.
- The devices are not managed by the NMS.

 Copyright © Huawei Technologies Co., Ltd.

- On RouterA, the ESN is 00080123456789, the MAC address is 0018-0303-1234, the system software name is **XXX-V200R010SPC100.cc** (XXX indicates the device model), and the version is V200R010. The configuration file to be loaded is **system-config01.zip**, the Android configuration file to be loaded is **settings.zip**, the resource file is **resource01.zip**, and the executable file is **execute01.sh** and needs to be executed after RouterA is upgraded successfully using a USB flash drive. HMAC check needs to be performed for all files. The authentication password for USB-based deployment is **huawei123**.
- On RouterB, the ESN is 66680123456789, the MAC address is 0018-0303-5678, and the system software name is **XXX-V200R010SPC100.cc**, and the version is V200R010. The configuration file to be loaded is **system-config02.zip**, the Android configuration file to be loaded is **settings.zip**, the resource file is **resource02.zip**, and the executable file is **execute02.sh** and needs to be executed after RouterB is upgraded successfully using a USB flash drive. HMAC check needs to be performed for all files. The authentication password for USB-based deployment is **huawei123**.

Configuration Roadmap

The configuration roadmap is as follows:

1. Make an index file **USB_AR.ini**.
2. Copy the index file **USB_AR.ini** and two resource files (**resource01.zip** and **resource02.zip**) to the root directory of the USB flash drive, and copy deployment files **XXX-V200R010SPC100.cc**, **settings.zip**, **execute01.sh**, **execute02.sh**, **system-config01.zip**, and **system-config02.zip** to the directory specified in the index file.
3. Connect the USB flash drive to a USB port of each device to complete automatic software upgrade.

   NOTE

   Before USB-based deployment, software engineers need to make an index file, save the index file to the root directory of a USB flash drive, save deployment files to the directory specified in the index file, and then deliver the USB flash drive to hardware installation engineers. After finishing installing devices onsite, hardware installation engineers insert the USB flash drive to the device to start the deployment process.

Procedure

Step 1 Edit the index file **USB_AR.ini**.

Use the authentication password as the key and use a file checker to calculate an HMAC for all deployment files based on the HMAC-SHA256 algorithm. The commonly used file checker is HashCalc, which is available at the website http://hashcalc.software.informer.com/download/. The calculation results are as follows:

- HMAC for the system software package of RouterA: 0ab30a2596bd0f6744631002d941f4218f40e784ae51447ed0bf3a2ff075939a
- HMAC for the configuration file of RouterA: c76b15e47346299b4993ea34d505e19844a04436dafcafe7a79341ef90a0652f
- HMAC for the Android configuration file of RouterA: c76a15e47346299b4993ea34d505e19844a04436dafcafe7a79341ef90a0652f

 Copyright © Huawei Technologies Co., Ltd.

- HMAC for the executable file of RouterA: c86b15e47346299b4993ea34d505e19844a04436dafcafe7a79341ef90a0652f
- HMAC for the resource file of RouterA: 0ab50a2596bd0f6744631002d941f4218f40e784ae51447ed0bf3a2ff075939a
- HMAC for the system software package of RouterB: 0ab30a2596bd0f6744631002d941f4218f40e784ae51447ed0bf3a2ff075939a
- HMAC for the configuration file of RouterB: 10736ef141ab2b6f9fa60a44c515cbb48c52d1b4b2e10f64abe5f880346e3b5d
- HMAC for the Android configuration file of RouterB: 16736ef141ab2b6f9fa60a44c515cbb48c52d1b4b2e10f64abe5f880346e3b5d
- HMAC for the executable file of RouterB: c86b15e47346299b4993ea34d505e19844a04436dafcafe7a79341ef90a0652f
- HMAC for the resource file of RouterB: 0ac30a2596bd0f6744631002d941f4218f40e784ae51447ed0bf3a2ff075939a

Create an index file and name it **USB_AR.ini**. Add the following content in the index file:

```
BEGIN AR
[USB CONFIG]
SN=20141008.080910
EMS_ONLINE_STATE=NO
[UPGRADE INFO]
OPTION=AUTO
DEVICENUM=2
[DEVICE1 DESCRIPTION]
OPTION=OK
ESN=00080123456789
MAC=0018-0303-1234
VERSION=V200R010
DIRECTORY=DEFAULT
FILENUM=5
TYPE1=SYSTEM-SOFTWARE
FILENAME1=XXX-V200R010SPC100.cc
FILE_HMAC1=0ab30a2596bd0f6744631002d941f4218f40e784ae51447ed0bf3a2ff075939a
TYPE2=SYSTEM-CONFIG
FILENAME2=system-config01.zip
FILE_HMAC2=c76b15e47346299b4993ea34d505e19844a04436dafcafe7a79341ef90a0652f
TYPE3=SYSTEM-CONFIG
FILENAME3=settings.zip
FILE_HMAC3=c76a15e47346299b4993ea34d505e19844a04436dafcafe7a79341ef90a0652f
EXECUTE_TIME1=1
TYPE4=SYSTEM-EXECUTE
FILENAME4=execute01.sh
FILE_HMAC4=c86b15e47346299b4993ea34d505e19844a04436dafcafe7a79341ef90a0652f
RESOURCE_NAME1=resource01.zip
RESOURCE_HMAC1=0ab50a2596bd0f6744631002d941f4218f40e784ae51447ed0bf3a2ff075939a
[DEVICE2 DESCRIPTION]
OPTION=OK
ESN=66680123456789
MAC=0018-0303-5678
VERSION=V200R010
DIRECTORY=DEFAULT
FILENUM=5
TYPE1=SYSTEM-SOFTWARE
FILENAME1=XXX-V200R010SPC100.cc
FILE_HMAC1=0ab30a2596bd0f6744631002d941f4218f40e784ae51447ed0bf3a2ff075939a
TYPE2=SYSTEM-CONFIG
FILENAME2=system-config02.zip
FILE_HMAC2=10736ef141ab2b6f9fa60a44c515cbb48c52d1b4b2e10f64abe5f880346e3b5d
TYPE3=SYSTEM-CONFIG
FILENAME3=settings.zip
FILE_HMAC3=16736ef141ab2b6f9fa60a44c515cbb48c52d1b4b2e10f64abe5f880346e3b5d
```

 Copyright © Huawei Technologies Co., Ltd.

```
EXECUTE_TIME1=1
TYPE4=SYSTEM-EXECUTE
FILENAME4=execute02.sh
FILE_HMAC4=c86b15e47346299b4993ea34d505e19844a04436dafcafe7a79341ef90a0652f
RESOURCE_NAME1=resource02.zip
RESOURCE_HMAC1=c86b15e47346299b4993ea34d505e19844a04436dafcafe7a79341ef90a0652f
END AR
```

Step 2 Copy the index file, system software, the executable file, the Android configuration file to be loaded, the configuration file and the resource file to the root directory of the USB flash drive.

Step 3 Configure an authentication password for USB-based deployment on the two devices.

Configure RouterA.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] set usb autoupdate password huawei123
```

Configure RouterB.

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] set usb autoupdate password huawei123
```

Step 4 Enable HMAC check on the two devices.

Configure RouterA.

```
[RouterA] hmac enable
```

Configure RouterB.

```
[RouterB] hmac enable
```

Step 5 Enable the USB-based deployment function on the two devices.

Configure RouterA.

```
[RouterA] autoupdate enable
```

Configure RouterB.

```
[RouterB] autoupdate enable
```

Step 6 Connect the USB flash drive to a device and start the upgrade process. (Connect the USB flash drive to the other device after completing the upgrade of the first device.)

Step 7 Observe the indicator on the USB flash drive to monitor the deployment state.

- If the deployment files do not exist, the indicator is off.
- If the deployment files exist but are invalid, USB-based deployment fails and the indicator is steady red.
- If valid deployment files exist but cannot be executed, USB-based deployment fails and the indicator is steady red.
- If valid deployment files exist and can be executed, USB-based deployment starts and the indicator blinks green.

  During the deployment, the system obtains the required files according to content in the index file (**USB_AR.ini**) and saves the files in the default storage medium. Then the device specifies the new system software and configuration file as the files for next startup, and restarts.

 Copyright © Huawei Technologies Co., Ltd.

Step 8 Verify the configuration.

After the device restarts, the system checks the deployment state. If the deployment indicator is steady green, USB-based deployment succeeds.

NOTE

After the USB-based deployment succeeds, remove the USB flash drive.

Run the **display usb** *usb-id* **autoupdate state** command to check the progress of USB-based deployment.

```
<RouterA> display usb 1 autoupdate state
Info: Deployment using the USB flash drive is completed successfully.
<RouterB> display usb 1 autoupdate state
Info: Deployment using the USB flash drive is completed successfully.
```

----End

 Copyright © Huawei Technologies Co., Ltd.

5 SMS-based Deployment Configuration

About This Chapter

Short message service (SMS)-based deployment allows 3G/LTE-supporting devices to activate 3G/LTE links and to be deployed by receiving deployment short messages. This method simplifies the deployment process and reduces deployment costs.

5.1 Overview of SMS-based deployment
This section describes the definition and purpose of SMS-based deployment.

5.2 Understanding SMS-based Deployment
This section describes how SMS-based deployment is implemented.

5.3 Application Scenarios for SMS-based Deployment
This section describes application scenarios for SMS-based deployment.

5.4 Licensing Requirements and Limitations for SMS-based Deployment

5.5 Default Settings for SMS-based Deployment
This section describes the default settings for SMS-based deployment.

5.6 Configuring SMS-based Deployment
This section describes how to configure SMS-based deployment.

5.7 Configuration Examples for SMS-based Deployment
This section provides an example of SMS-based deployment, including networking requirements, configuration roadmap, and configuration procedure.

5.1 Overview of SMS-based deployment

This section describes the definition and purpose of SMS-based deployment.

Definition

Deployment personnel send deployment short messages to 3G/LTE-supporting devices. The devices then obtain and parse the short messages to activate 3G/LTE

 Copyright © Huawei Technologies Co., Ltd.

links, and obtain and load a configuration file from a file server. This deployment method can implement zero touch deployment of the devices in a batch.

Purpose

As the number of branches in enterprises keeps increasing, more branch devices need to be deployed on enterprise networks. However, these branch devices cannot be deployed uniformly because they are geographically dispersed and difficult or fail to obtain wired communications resources. As a result, deployment personnel often need to configure software for branch devices one by one onsite, increasing deployment costs and reducing deployment efficiency.

Huawei offers SMS-based deployment function to solve this problem. This function only requires deployment personnel to send deployment short messages to branch devices, which then receive and parse the short messages and connect to enterprise networks in 3G/LTE mode to active 3G/LTE links. Branch devices can work with eSight network management system (NMS) and SMS gateways to obtain a configuration file from a file server and load the files for zero touch deployment in a batch. This function simplifies the deployment process and reduces deployment costs.

5.2 Understanding SMS-based Deployment

This section describes how SMS-based deployment is implemented.

Implementation

Before SMS-based deployment, enterprise network administrators save the configuration file of devices to a specified file server. Devices need to be installed and powered on before they can receive and parse deployment short messages. According to the short messages, devices can obtain parameter information to activate 3G/LTE links, and connect to the NMS or the file server to obtain and load a configuration file for zero touch deployment.

When eSight is deployed in the enterprise headquarters to manage devices, enterprise network administrators send deployment short messages to devices through eSight after obtaining device information.

NOTE

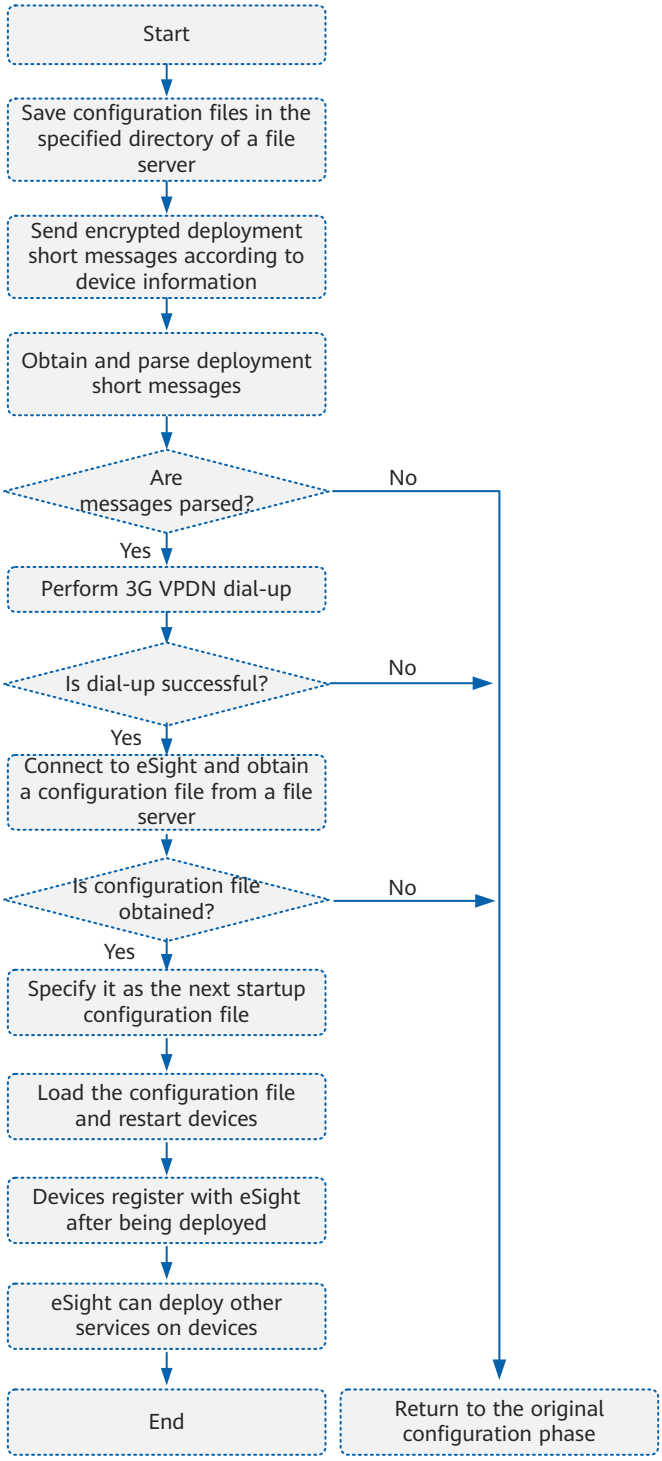
Deployment short messages and parameter information are transmitted over a carrier network. All the transmitted information will be encrypted using Advanced Encryption Standard (AES) 128 or Rivest-Shamir-Adleman (RSA) algorithm to ensure data security.

SMS-based Deployment Process

Figure 5-1 illustrates the SMS-based deployment process when eSight is available.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-1 Device running flowchart during SMS-based deployment (when eSight is available)



The device running process involves the following phases:

1. Enterprise network administrators save configuration files in the specified directory of a file server.
2. Enterprise network administrators obtain device information and SIM card information and then send encrypted deployment short messages through NMS.

 Copyright © Huawei Technologies Co., Ltd.

3. Parse deployment short messages.

   Devices receive and parse deployment short messages to obtain parameter information. The short messages carry the following information:

   a. SIM card information: includes International Mobile Subscriber Identity (IMSI) and Access Point Name (APN) activation information (including the APN, user name, and password).

   b. NMS parameter information: includes the eSight server address.

   NOTE

   Deployment short messages are encrypted using AES128 algorithm to ensure user information security.

4. Activate 3G/LTE links.

   Devices dial up to the enterprise network according to the APN activation information obtained from the parsed deployment short messages. If the dial-up is successful, they connect to the enterprise network over a 3G/LTE network, and obtain IP addresses after passing authentication.

5. Obtain and load a configuration file.

   a. Devices connect to eSight and send deployment registration requests.

      After devices obtain IP addresses, they connect to eSight and send deployment registration requests to it. eSight authenticates the deployment registration requests. After successful authentication, eSight returns file server parameter information, including the file server IP address, user name, and password.

      NOTE

      The file server parameter information is encrypted using RSA algorithm to ensure data security.

   b. Devices connect to the file server to obtain and load a configuration file.

      After devices obtain file server information, they connect to the file server through SFTP, and then download and load the specified configuration file. Configurations take effect on the devices after these devices restart.

      NOTE

      Devices will send status notifications to eSight regardless of whether they download a configuration file successfully. If devices cannot download the configuration file, they send the failure reason to eSight for fault location.

6. Register.

   Devices connect to eSight again for registration after configurations take effect. After devices have registered, enterprise network administrators can deploy other services on the devices through eSight, including upgrading the devices and load patches on the devices.

5.3 Application Scenarios for SMS-based Deployment

This section describes application scenarios for SMS-based deployment.

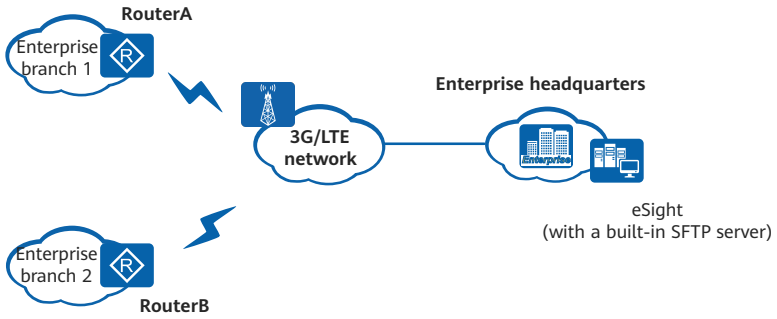
SMS-based deployment function implements zero touch deployment of devices. When devices are managed by eSight, network administrators can send

 Copyright © Huawei Technologies Co., Ltd.

deployment short messages to devices through eSight to complete zero touch deployment of the devices in a batch.

In **Figure 5-2**, Branch routers in different locations (such as routers placed within off-bank ATMs) connect to the enterprise headquarters over the Internet through 3G/LTE links. RouterA and RouterB function as egress gateways of enterprise branches, and eSight (with a built-in SFTP server) is deployed on the enterprise headquarters to send deployment short messages to devices.

Figure 5-2 SMS-based deployment through eSight



Onsite installation personnel install devices and then send device information to enterprise network administrators. According to the received device information, the administrators send deployment short messages to devices through eSight. Devices receive and parse the short messages, connect to eSight over the 3G/LTE network, and download as well as load a configuration file from a file server. This method implements device registration and zero touch deployment. After device deployment is completed, the administrators can upgrade these devices or deploy other services on these devices through eSight.

5.4 Licensing Requirements and Limitations for SMS-based Deployment

Involved Network Elements

None

Licensing Requirements

SMS-based deployment is a basic feature of a router and is not under license control.

Feature Limitations

3G/LTE-supporting devices support SMS-based deployment. However, the AR109, AR109W, AR109GW-L, AR129CV, AR129CVW, and AR129CGVW-L do not support this function.

 Copyright © Huawei Technologies Co., Ltd.

- Currently, 3G-supporting devices include:
  - 3G/LTE routers, which need to have 3G/LTE antennas installed before being used. For specific device models, see Licensing Requirements and Limitations for 3G Cellular Interfaces in "3G Cellular Interface Configuration".
  - Routers that can have 3G cards (except 3G-EVDO cards) installed in SIC slots. For specific device models, see Licensing Requirements and Limitations for 3G Cellular Interfaces in "3G Cellular Interface Configuration".
- Currently, the following routers support the LTE functions:
  - 3G/LTE routers, which need to have 3G/LTE antennas installed before being used. For specific device models, see Overview of LTE Cellular Interfaces in "LTE Cellular Interface Configuration".
  - Routers that can have LTE interface cards installed in slots. For specific device models, see Licensing Requirements and Limitations for LTE Cellular Interfaces in "LTE Cellular Interface Configuration".

5.5 Default Settings for SMS-based Deployment

This section describes the default settings for SMS-based deployment.

Table 5-1 Default settings for SMS-based deployment

Parameter	Default Setting
SMS-based deployment	Enabled

5.6 Configuring SMS-based Deployment

This section describes how to configure SMS-based deployment.

5.6.1 Configuring SMS-based Deployment

This section describes the process of configuring SMS-based deployment through eSight.

Pre-configuration Tasks

- Onsite installation personnel install, power on, and perform self-check on devices.
- Enterprise network administrators obtain device information and SIM card information.
- Devices support 3G/LTE functions and have SIM cards installed. Ensure that areas where devices reside have 3G/LTE signals.
- eSight can send messages normally.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

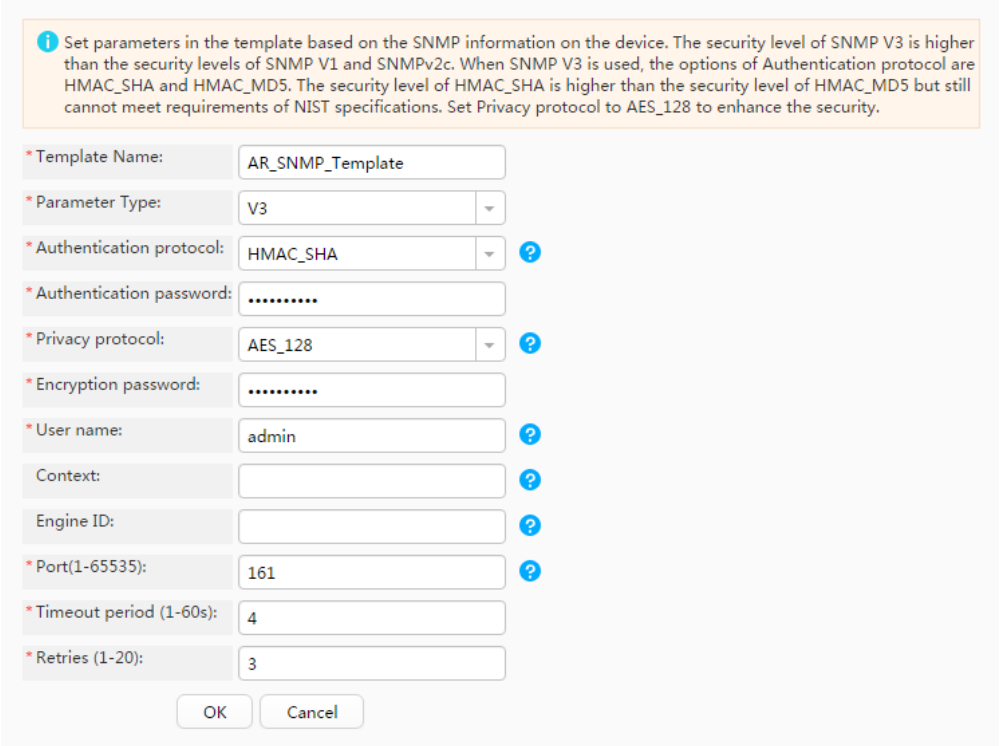
Step 1 Create an SNMP template.

Log in to eSight, and choose **Resource** > **Protocol Template** > **SNMP Template**. The **SNMP Template** page is displayed. Click **Create** to create an SNMP template, as shown in **Figure 5-3**. Configure the SNMP template according to the SNMP version. You are advised to configure **Template Name** and **Parameter Type** before configuring other parameters, as shown in **Table 5-2**. Click **OK** to save the configuration.

NOTE

- SMS-based deployment requires high security, so SNMPv3 is recommended.
- Configure parameters in the SNMP template according to SNMP information on devices. When using SNMPv3, you are advised to set **Privacy protocol** to AES_128 to improve security because authentication protocols HMAC_SHA and HMAC_MD5 cannot ensure high security.

Figure 5-3 Creating an SNMP template



 Copyright © Huawei Technologies Co., Ltd.

Table 5-2 Parameters

Parameter	Description
Parameter Type	Specifies an SNMP version: ● V1: SNMPv1 ● V2c: SNMPv2c ● V3: SNMPv3, which applies to scenarios requiring high security
Authentication protocol	Specifies the protocol used to authenticate messages, which can be HMAC_SHA or HMAC_MD5. **NOTE** ● HMAC_MD5 may have information security risks. HMAC_SHA is more secure and so is recommended. ● This parameter can be configured only when **Parameter Type** is set to SNMPv3.
Authentication password	Specifies the authentication password. **NOTE** ● When using HMAC_MD5 or HMAC_SHA, you need to set an authentication password. ● This parameter can be configured only when **Parameter Type** is set to SNMPv3.
Privacy protocol	Specifies the encryption protocol used in data encapsulation, which can be CBC_DES or AES_128. **NOTE** ● CBC_DES may have information security risks. AES_128 is more secure and so is recommended. ● This parameter can be configured only when **Parameter Type** is set to SNMPv3.
Encryption password	Specifies the encryption password used in data encapsulation. **NOTE** ● This parameter needs to be configured when **Privacy protocol** is CBC_DES or AES_128. ● This parameter can be configured only when **Parameter Type** is set to SNMPv3.
User name	Specifies the login user name. **NOTE** This parameter can be configured only when **Parameter Type** is set to SNMPv3.
Context	Specifies the context engine name. This parameter must be empty by default. If it needs to be modified, ensure that it is consistent with that on devices. **NOTE** This parameter can be configured only when **Parameter Type** is set to SNMPv3.

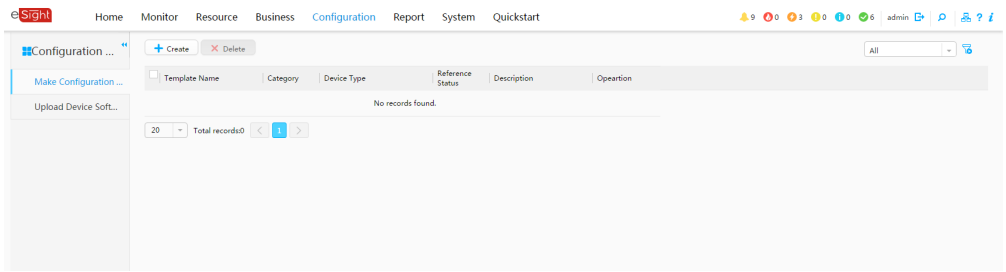
 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Engine ID	Specifies the entity engine ID. To view the context engine ID on a device, run the **display snmp-agent local-engineid** command on the device.
Port	Specifies the SNMP port.
Timeout period	Specifies the time during which eSight waits for a response to an operation request.
Retries	Specifies the maximum number of times eSight resends an operation request upon timeout events. If eSight does not receive any response after sending the request the maximum number of times, eSight considers that this operation fails.

Step 2 Create a configuration template.

1. Log in to eSight, and choose **Configuration** > **Zero Touch Provisioning** > **Configuration File Making**. The **Configuration File Making** page is displayed, as shown in **Figure 5-4**.

   Figure 5-4 Making a version file

2. Choose **Make Configuration Template** and click **Create** to set parameters in the configuration template, as shown in **Figure 5-5**. Select **Router** from the **Device Type** drop-down list box, and click ... to select the device type, as shown in **Figure 5-13**. Set parameters in the configuration template according to service requirements, as shown in **Table 5-3**. Click **Next** to save the configuration, as shown in **Figure 5-6**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-5 Making a configuration template (1)

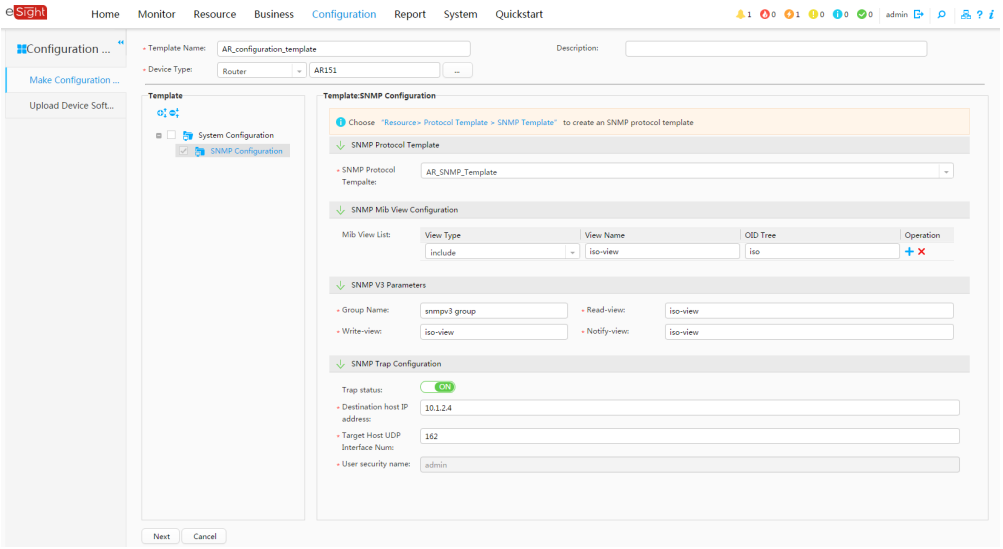
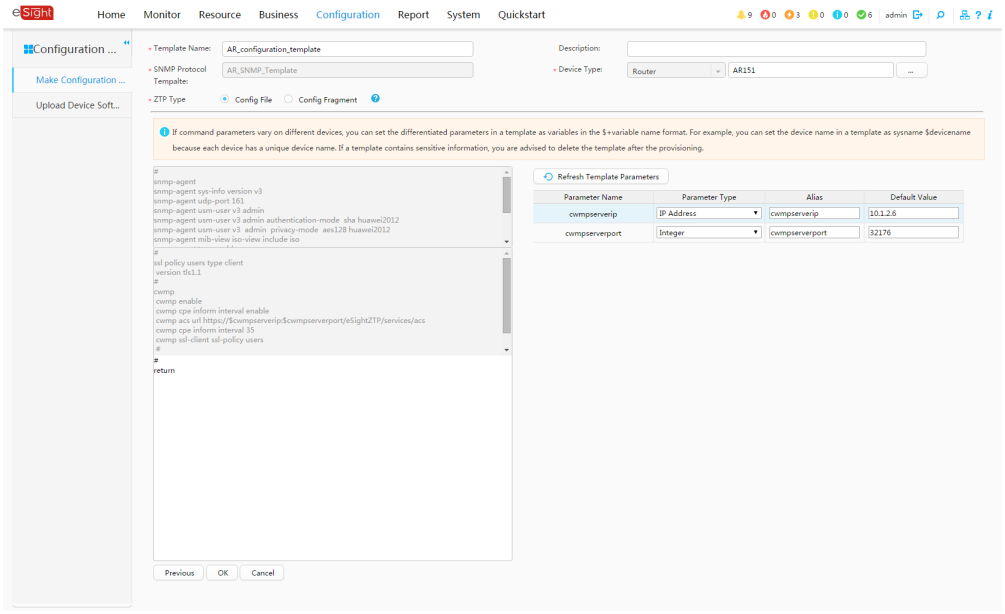


Table 5-3 Parameters

Parameter	Description
Template Name	Specifies the configuration template name.
Description	Specifies a description for the configuration template.
Device Type	Specifies the type of devices to be deployed.
SNMP Protocol Template	Specifies the SNMP template.
SNMP Mib View Configuration	Indicates SNMP MIB view parameter information, including the type, SNMP view name, and OID/MIB subtree.
SNMP V3 Parameters	Indicates SNMPv3 parameter information, including group name, read view, write view, and notify view.
SNMP Trap Configuration	Indicates SNMP trap configuration. If you click **ON**, the SNMP trap function is enabled. Parameters include: – Destination host IP address – Destination host UDP port number – User security name

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-6 Making a configuration template (2)



3. Click **OK** to save the made configuration template.

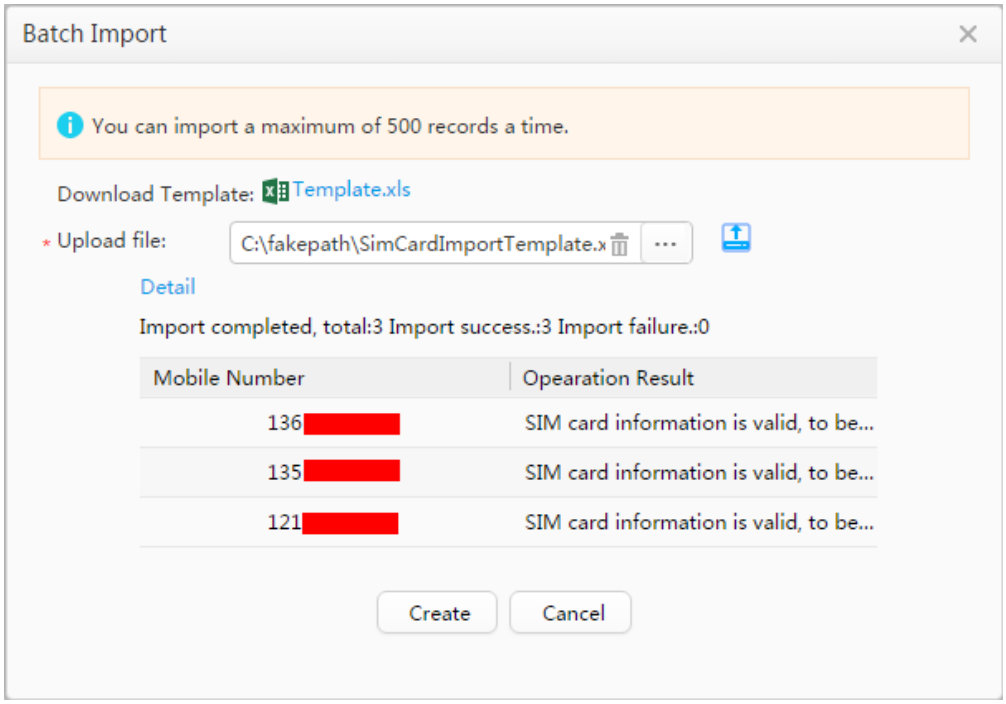
Step 3 Create SIM card information and short messages.

1. Choose **Configuration** > **Zero Touch Provisioning** > **Short Message-based Provisioning** > **Manage SIM Card**. The **Manage SIM Card** page is displayed.

   Click **Batch Import** to import SIM card information in a batch, as shown in **Figure 5-7**. Click **Template.xls** to download a template, and then enter multiple mobile phone numbers and IMSIs in the template. Click ... to select the template file to be uploaded. Click to upload the template file. After the template file has been uploaded, view the import results under **Detail**. Click **Create** to finish batch import.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-7 Batch import



2. Choose **Short Message-based Provisioning** > **Manage Short Message**. The **Manage Short Message** page is displayed. Click **Create** and configure parameters in the displayed dialog box, as shown in **Table 5-4**. Click **OK** to save the configuration, as shown in **Figure 5-8**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-8 Creating short messages

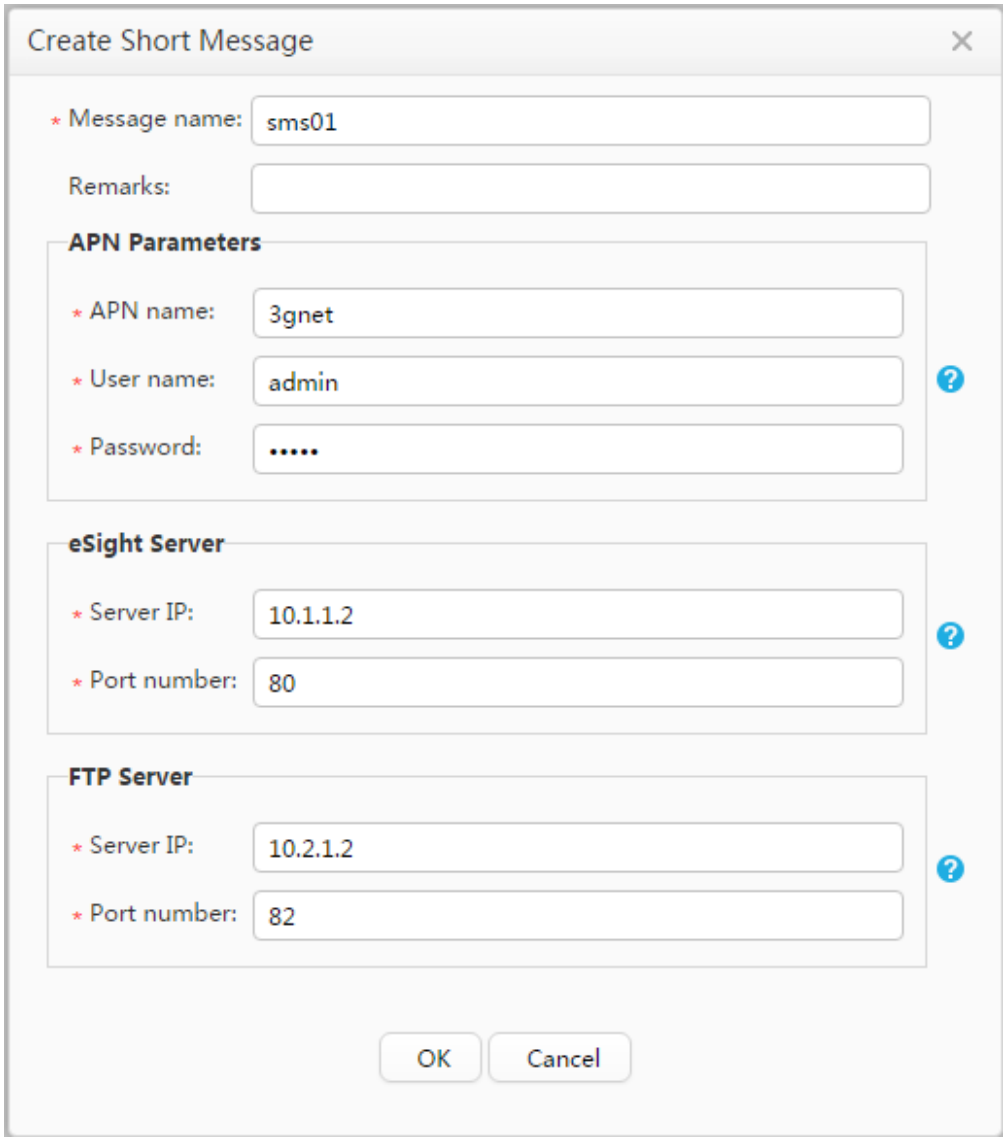


Table 5-4 Parameters

Parameter	Description
Message name	Specifies the short message name.
APN name	Specifies the APN used to identify the GPRS service type. **NOTE** – APNs are provided by carriers. – For example, APNs of China Mobile, China Telecom, and China Unicom are CMNET, CTNET, and 3GNET respectively.

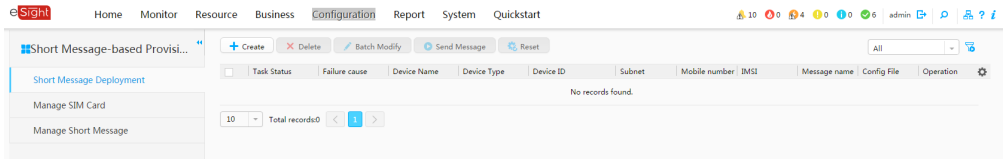
 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
User name	Specifies the user name for 3G/LTE dial-up. **NOTE** User names can be obtained from carriers.
Password	Specifies the password for 3G/LTE dial-up. **NOTE** Passwords can be obtained from carriers.
Service IP (eSight Server)	Specifies the eSight server IP address.
Port number (eSight Server)	Specifies the eSight server port number.
Server IP (FTP Server)	Specifies the file server IP address.
Port number (FTP Server)	Specifies the file server port number.

Step 4 Configure SMS-based deployment.

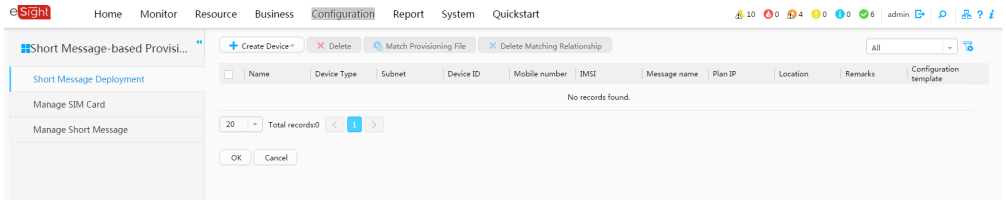
1. Choose **Configuration** > **Zero Touch Provisioning** > **Short Message Deployment**. The **Short Message Deployment** page is displayed, as shown in **Figure 5-9**.

Figure 5-9 Short message deployment (1)



2. Choose **Short Message Deployment** > **Create**. The short message creation page is displayed, as shown in **Figure 5-10**.

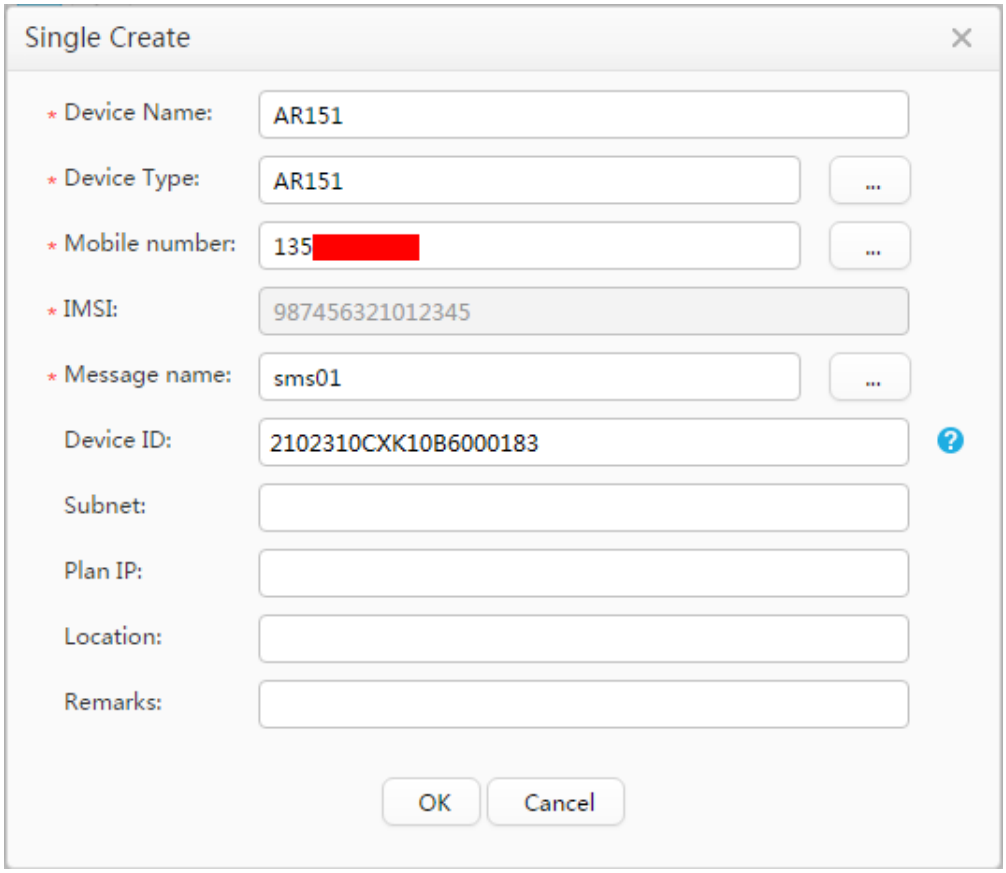
Figure 5-10 Short message deployment (2)



3. Click **Create Device** and select **Single Create** from the drop-down list. The **Single Create** page is displayed, as shown in **Figure 5-11**.

 Copyright © Huawei Technologies Co., Ltd.

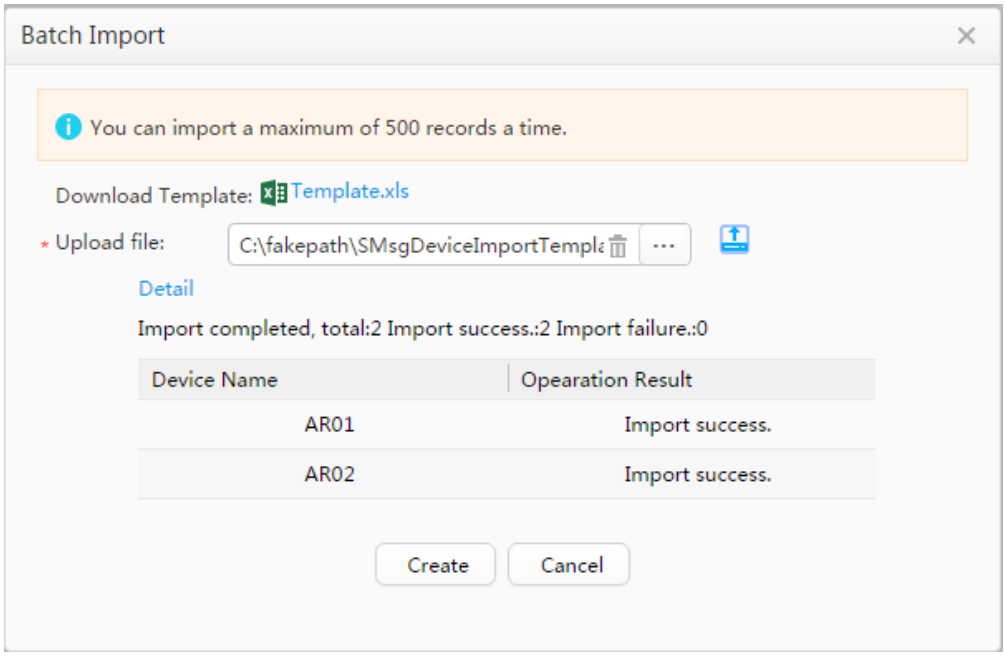
Figure 5-11 Single create



(Optional) Click **Batch Import** to import short message deployment information in a batch. Click **Template.xls** to download a template, and then enter short message deployment information in the template. Click ... to select the template file to be uploaded. Click to upload the template file. After the template file has been uploaded, view the import results under **Detail**. Click **Create** to finish batch import, as shown in **Figure 5-12**.

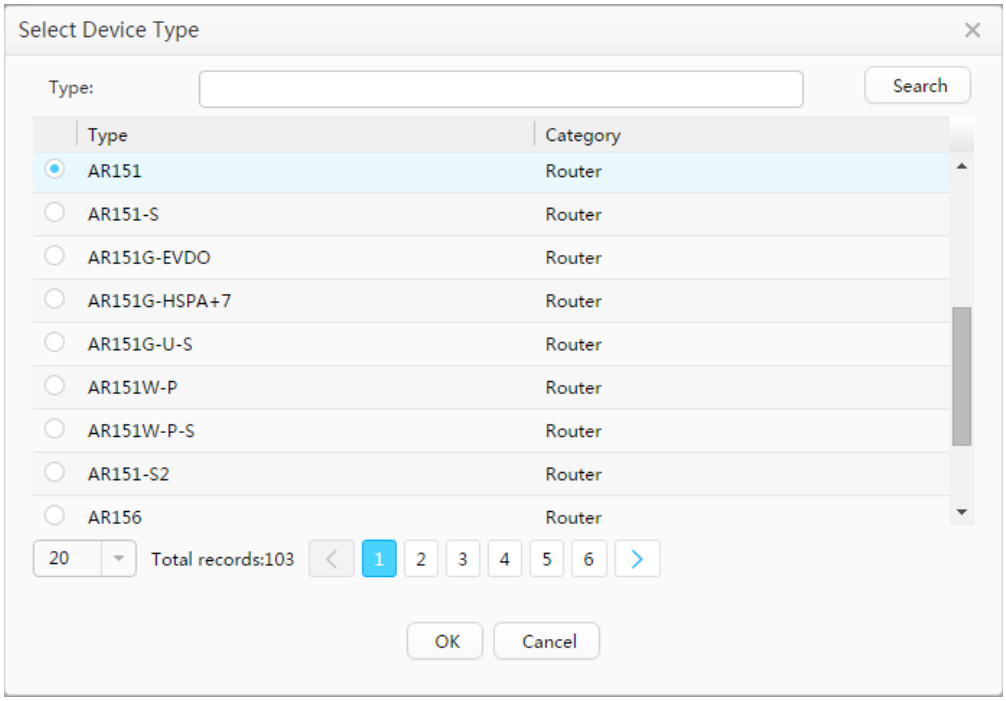
 Copyright © Huawei Technologies Co., Ltd.

Figure 5-12 Batch import



4. Enter information such as the device name and SIM card on the **Single Create** page. Click ... behind the **Device Type** text box. The **Select Device Type** page is displayed. Select the device types to be deployed, as shown in **Figure 5-13**. Click **OK** to save the configuration.

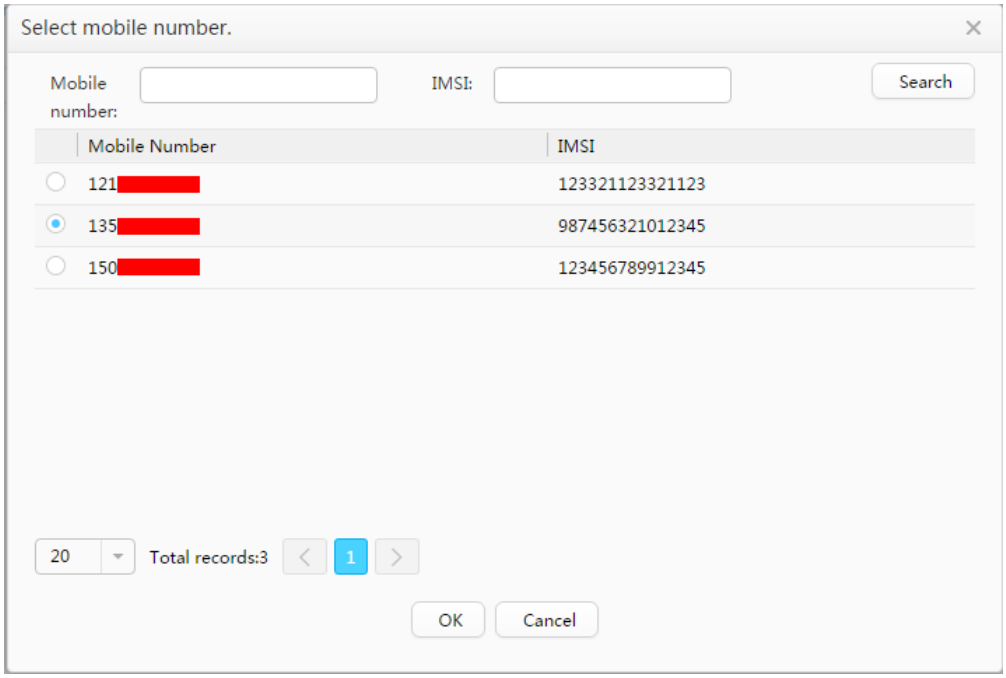
Figure 5-13 Select device type



 Copyright © Huawei Technologies Co., Ltd.

5. Click ... behind the **Mobile number** text box. The **Select mobile number** page is displayed. Select the imported mobile phone numbers, and click **OK** to save the configuration, as shown in **Figure 5-14**.

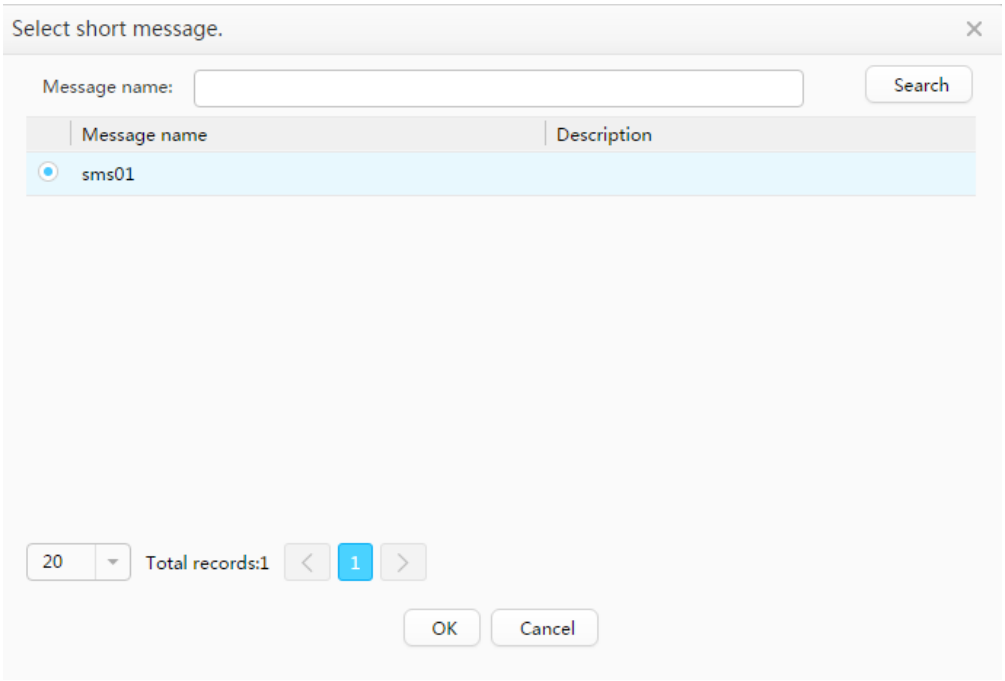
   Figure 5-14 Select mobile number



6. Click ... behind the **Message name** text box. The **Select short message** page is displayed. Select the created short messages, and click **OK** to save the configuration, as shown in **Figure 5-15**.

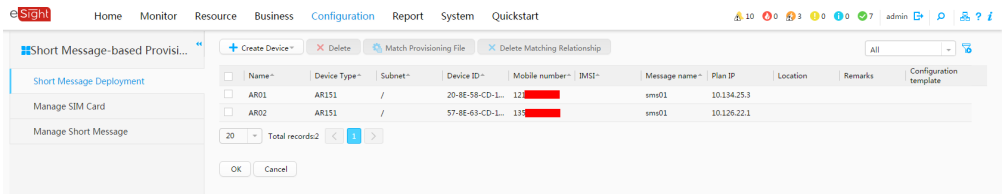
 Copyright © Huawei Technologies Co., Ltd.

Figure 5-15 Select short message



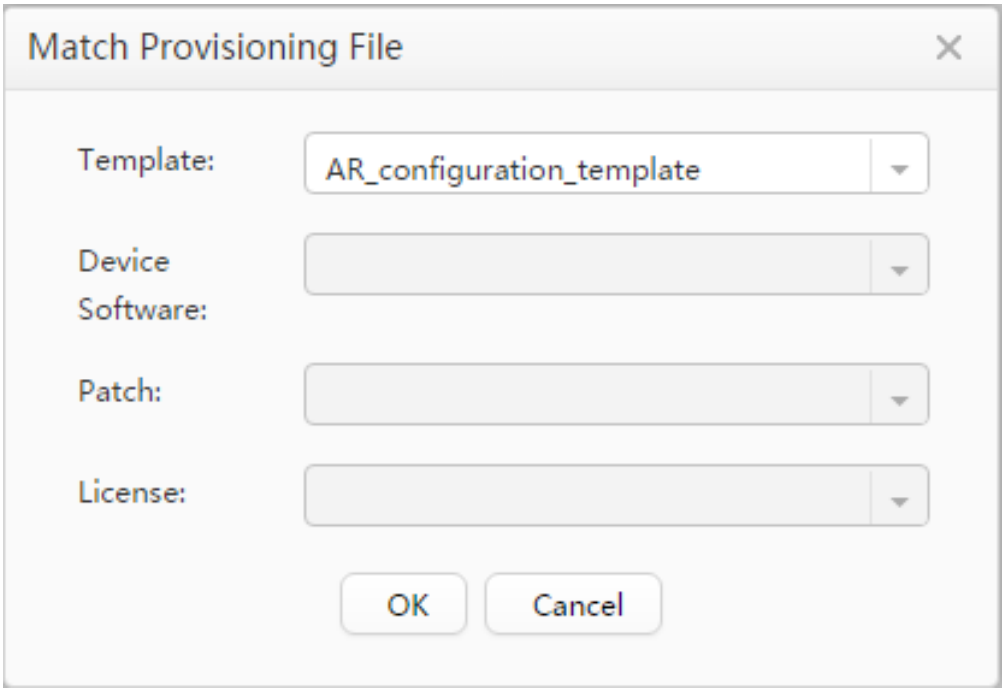
7. Click **OK** to save the configuration, and then the created short messages will be displayed on the **Short Message Deployment** page, as shown in **Figure 5-16**. Select the devices to be deployed and click **Match Provisioning File** to select the created configuration template, as shown in **Figure 5-17**. Click **OK** to save the configuration.

Figure 5-16 Created deployment information



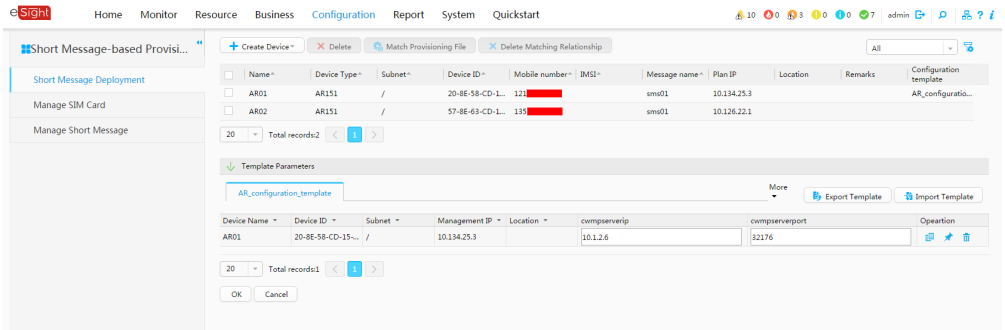
 Copyright © Huawei Technologies Co., Ltd.

Figure 5-17 Matching deployment files



8. After the configuration has been saved, information about the configuration template will be displayed on the **Short Message Deployment** page, as shown in **Figure 5-18**. Click **OK** to finish SMS-based deployment configuration.

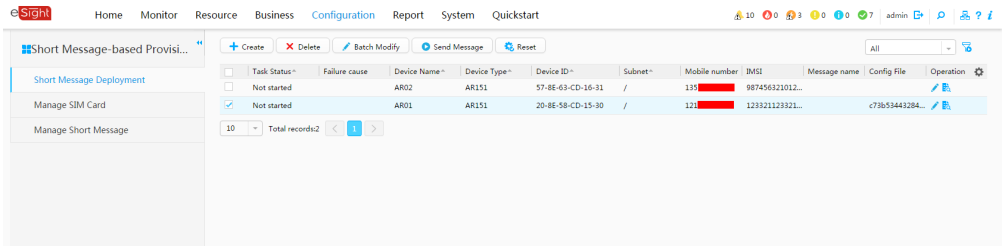
Figure 5-18 Short message deployment



9. Select the SMS-based deployment task and click **Send Message** for SMS-based deployment, as shown in **Figure 5-19**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-19 Sending messages



Step 5 (Option) Configure a mobile phone number whitelist.

After devices are deployed successfully, you can perform the following operations to allow modifying device configurations according to short messages sent from some mobile phone numbers:

1. Run the **system-view** command to enter the system view.
2. Run the **sms config caller** *tel-number* command to configure a mobile phone number whitelist.

   By default, no mobile phone number whitelist is configured.

   NOTE

   This step is recommended if you want to prevent device configurations from being modified according to short messages sent from unauthorized phone numbers. Subsequently, device configurations can be modified only according to short messages sent from phone numbers in the configured mobile phone number whitelist.

Step 6 (Optional) Run the **undo sms config autodeploy enable** command to disable SMS-based deployment.

By default, SMS-based deployment is enabled.

NOTE

After devices are deployed successfully, you are advised to disable SMS-based deployment to prevent unauthorized users from forging deployment short messages to modify device configurations.

----End

5.7 Configuration Examples for SMS-based Deployment

This section provides an example of SMS-based deployment, including networking requirements, configuration roadmap, and configuration procedure.

5.7.1 Example for Configuring SMS-based Deployment

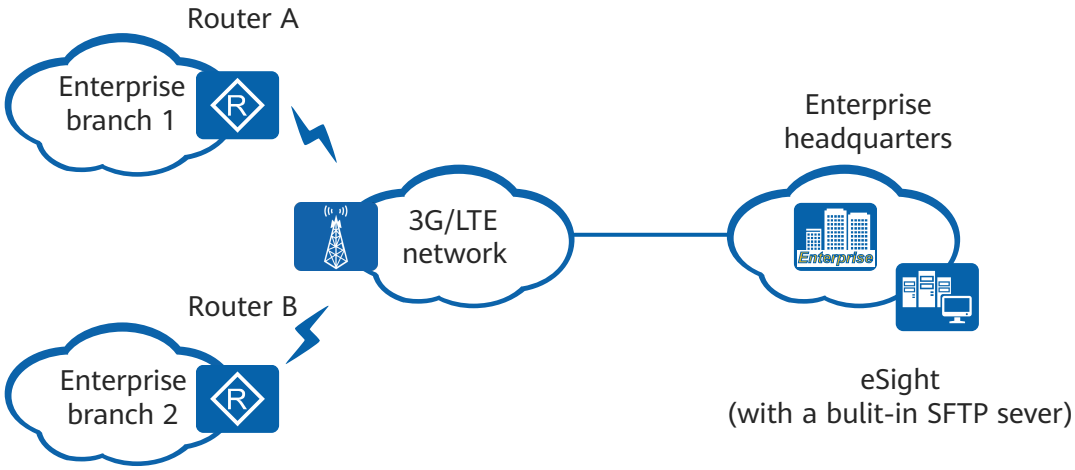
Networking Requirements

In **Figure 5-20**, eSight (with a built-in SFTP server) is deployed in the enterprise headquarters. Dispersed branch devices connect to eSight through 3G/LTE dial-up.

 Copyright © Huawei Technologies Co., Ltd.

The enterprise requires that branch devices are upgraded by onsite installation personnel when a large number of branch devices are geographically dispersed and difficult to obtain wired resources. Meanwhile, allow the mobile phone number with that segment 456789 matches this number segment to send short messages for SMS-based deployment. During deployment, devices can connect to the enterprise network over a 3G/LTE network, and enterprise network administrators can deploy devices through eSight.

Figure 5-20 Configuring SMS-based deployment



The following provides SIM card information and device information of RouterA.

- SIM card information: The IMSI is 987456321012345, the mobile phone number is 135XXXXXXXX, the APN is 3gnet, the dial-up user name is **admin**, and the dial-up password is **huawei123**.

  NOTE

  SIM card information can be obtained from carriers.

- Device information: The device type is AR151 and the device ESN is 2102310CXK10B6000183.

eSight information and file server information are as follows:

- eSight: The eSight server IP address is 10.1.2.3/24 and the port number is 32176.
- File server: The SFTP server IP address is 10.1.2.4/24 and the port number is 31922.

Configuration Roadmap

The configuration roadmap is as follows:

1. Save the configuration file to be loaded to branch devices to the SFTP server to ensure that the devices can obtain the configuration file.
2. Operate eSight, make a configuration template.
3. Operate eSight, edit deployment short messages.
4. Configure SMS-based deployment.
5. Configure a mobile phone number whitelist to allow configuring devices through mobile phone numbers in the whitelist.

 Copyright © Huawei Technologies Co., Ltd.

6. Disable SMS-based deployment to prevent unauthorized users from modifying device configurations using forged deployment short messages.

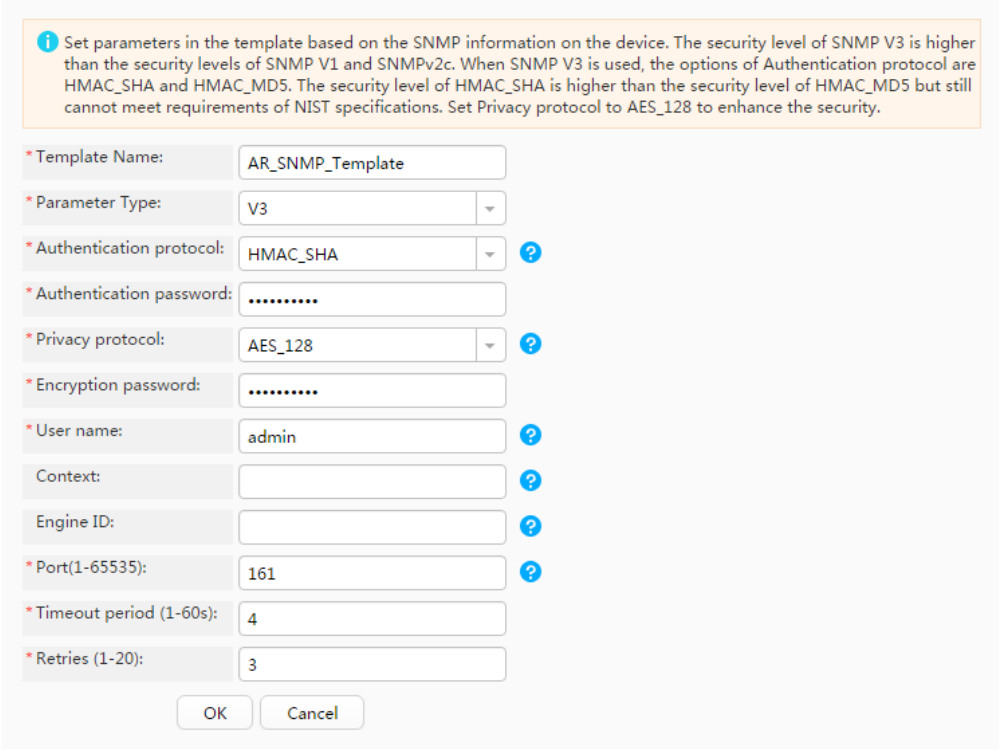
Procedure

Step 1 Save the configuration file to be loaded to branch devices to the SFTP server.

Step 2 Make a configuration template.

1. Log in to eSight, and choose **Resource** > **Protocol Template** > **SNMP Template**. The **SNMP Template** page is displayed. Click **Create** to create an SNMP template, as shown in **Figure 5-21**. Set the SNMP version type to SNMPv3, authentication protocol to HMAC_SHA, and privacy protocol to AES_128, and configure other parameters according to service requirements. Click **OK** to save the configuration.

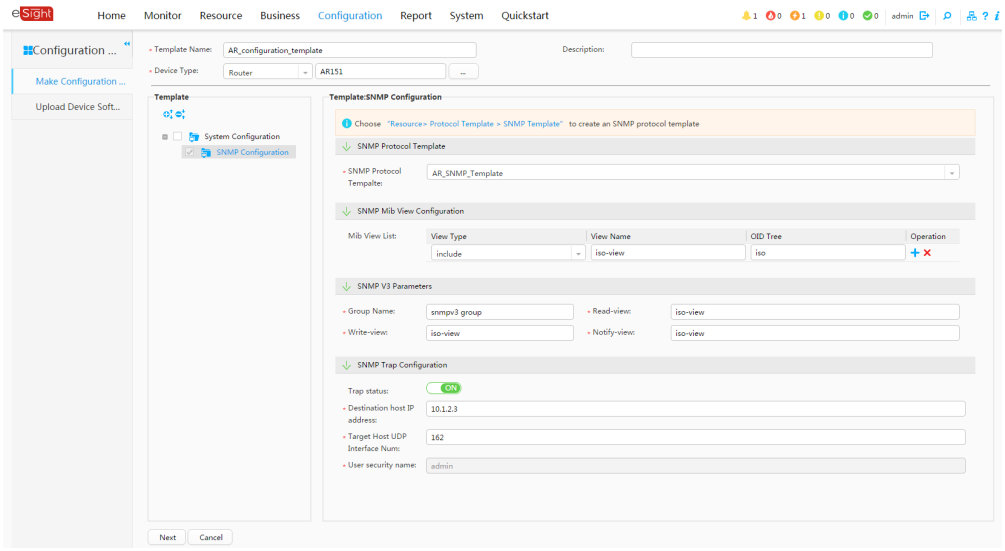
   Figure 5-21 Creating an SNMP template



2. Choose **Configuration** > **Zero Touch Provisioning** > **Configuration File Making** > **Make Configuration Template**. Click **Create**, and set **Template Name**, **Device Type**, and SNMP parameters, as shown in **Figure 5-22**.

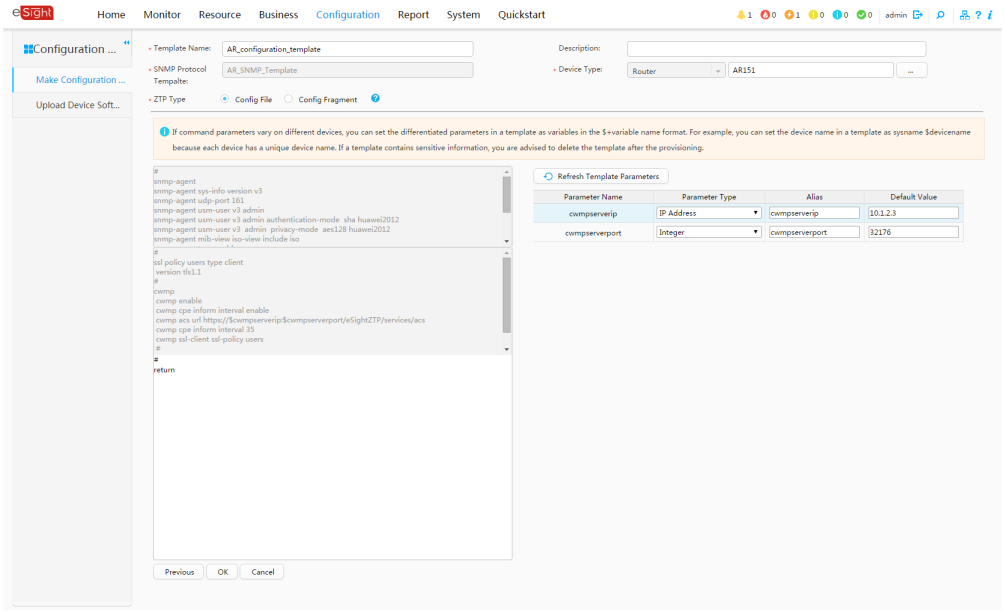
 Copyright © Huawei Technologies Co., Ltd.

Figure 5-22 Making a configuration template (1)



3. Click **Next** and set **ZTP Type** to **Config File**. Click **OK** to save the configuration, as shown in **Figure 5-23**.

Figure 5-23 Making a configuration template (2)



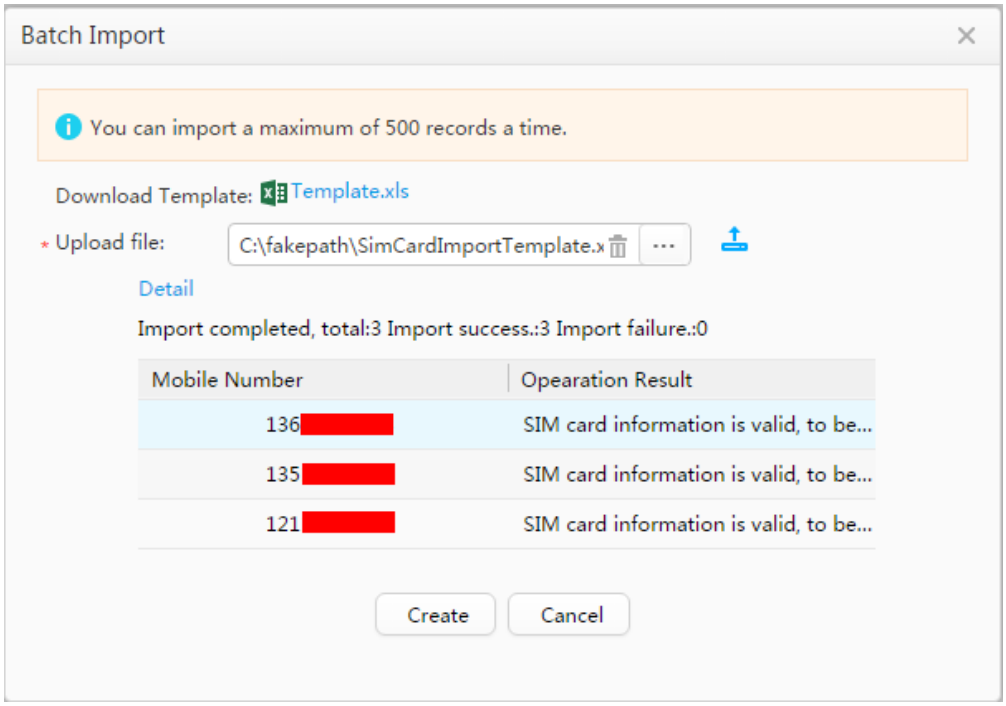
Step 3 Configure SIM card information and short message parameters.

1. Choose **Configuration** > **Zero Touch Provisioning** > **Short Message-based Provisioning** > **Manage SIM Card**. The **Manage SIM Card** page is displayed.

   Click **Batch Import** to import SIM card information in a batch. Click ... to select the template file to be uploaded. Click to upload the template

file. After the template file has been uploaded, view the import results under **Detail**. Click **Create** to finish batch import, as shown in **Figure 5-24**.

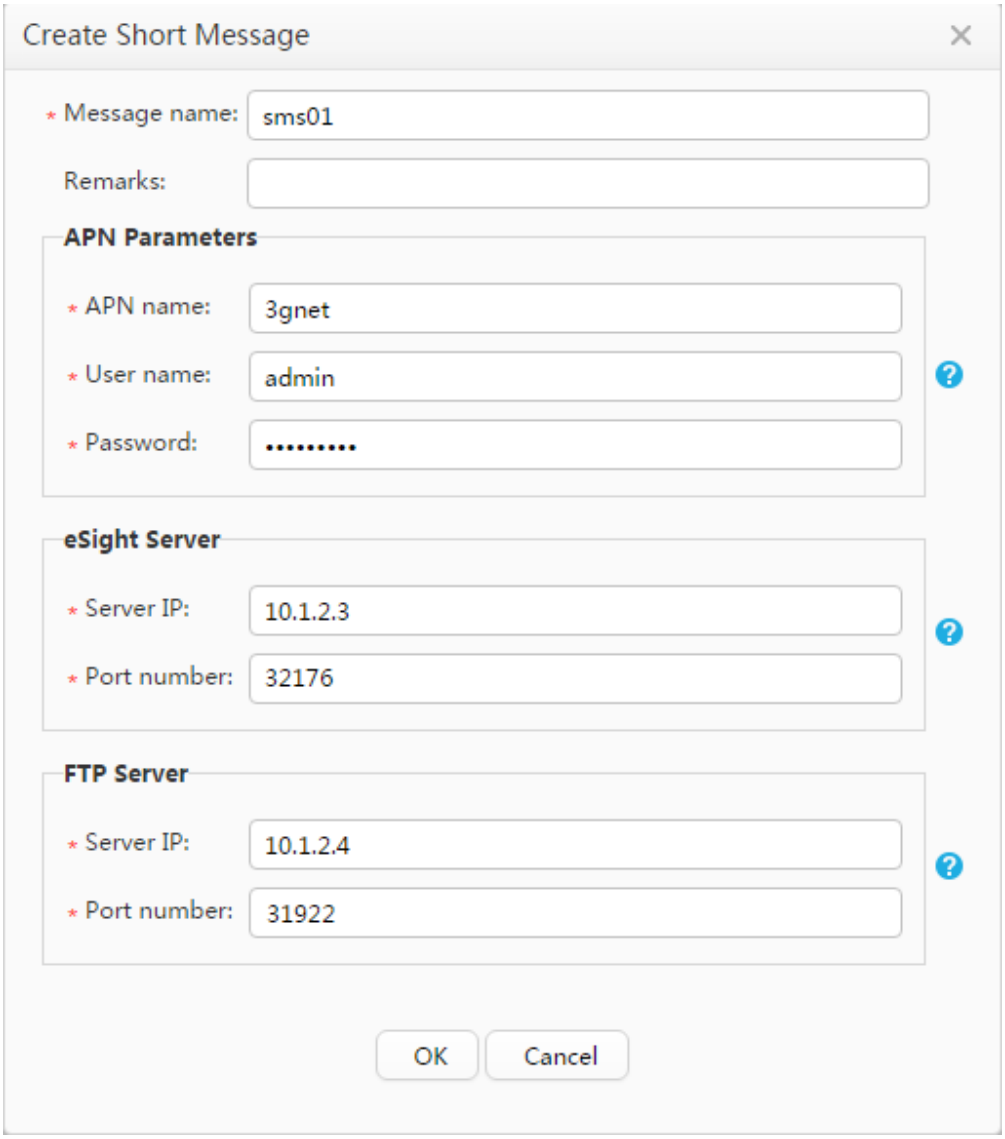
Figure 5-24 Batch import



2. Choose **Short Message-based Provisioning** > **Manage Short Message**. The **Manage Short Message** page is displayed. Click **Create** and enter short message parameter information in the displayed dialog box. Click **OK** to save the configuration, as shown in **Figure 5-25**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-25 Creating short messages



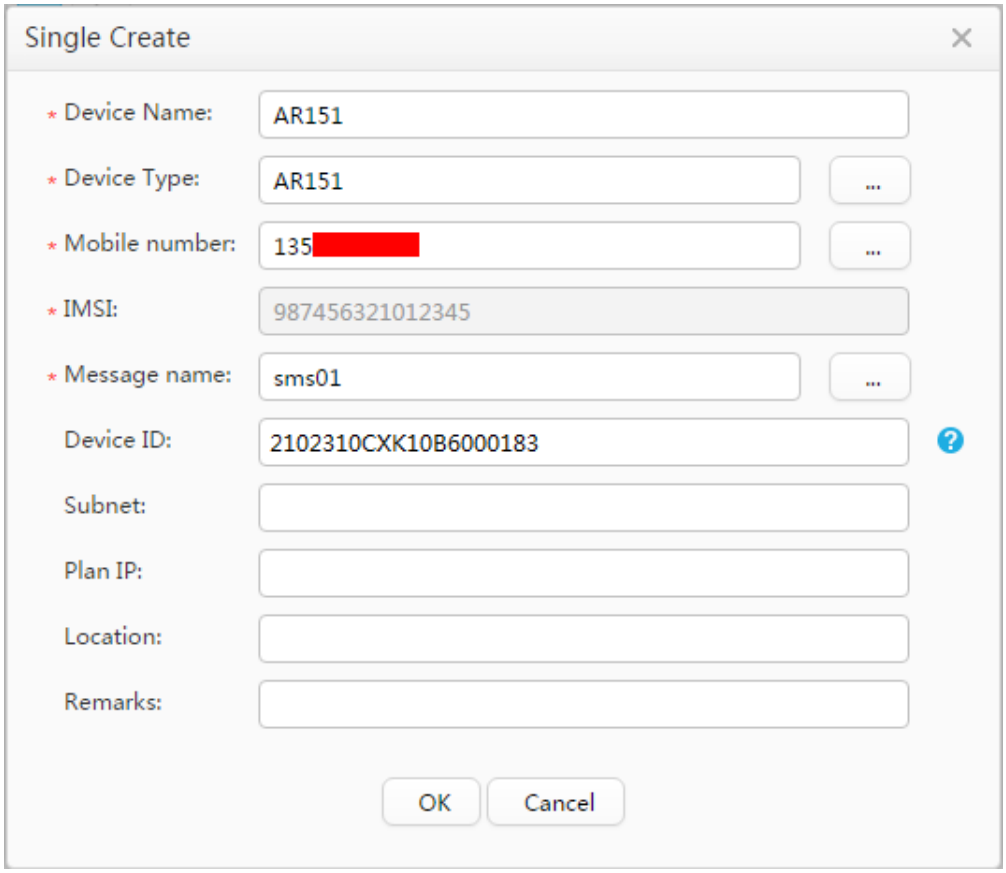
Step 4 Configure SMS-based deployment.

1. Choose **Short Message Deployment** > **Create**. The **Short Message Deployment** page is displayed. Click **Create Device**, select **Single Create** from the drop-down list, and enter device information and SIM card information in the displayed dialog box, as shown in **Figure 5-26**. Click ... behind the **Device Type** text box. The **Select Device Type** page is displayed. Select the device types to be deployed, as shown in **Figure 5-27**. Click ... behind the **Mobile number** text box. The **Select mobile number** page is displayed. Select the imported mobile phone number information, as shown in **Figure 5-28**. Click ... behind the **Message name** text box. The **Select short message** page is displayed. Select the

 Copyright © Huawei Technologies Co., Ltd.

created short messages, as shown in **Figure 5-29**. Click **OK** to save the configuration.

Figure 5-26 Single create



 Copyright © Huawei Technologies Co., Ltd.

Figure 5-27 Select device type

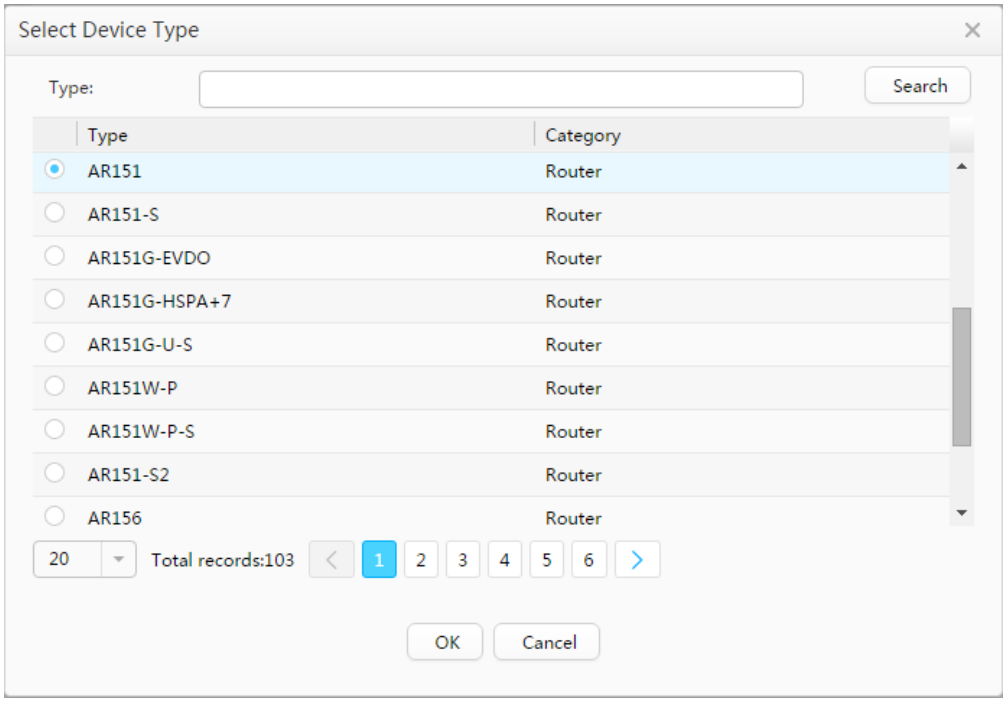
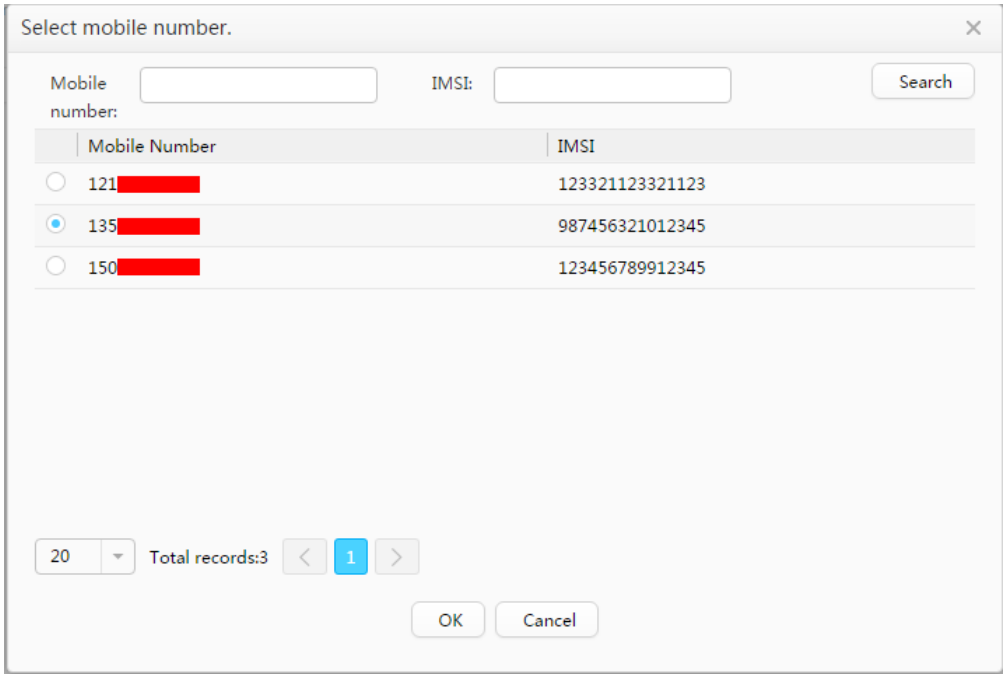
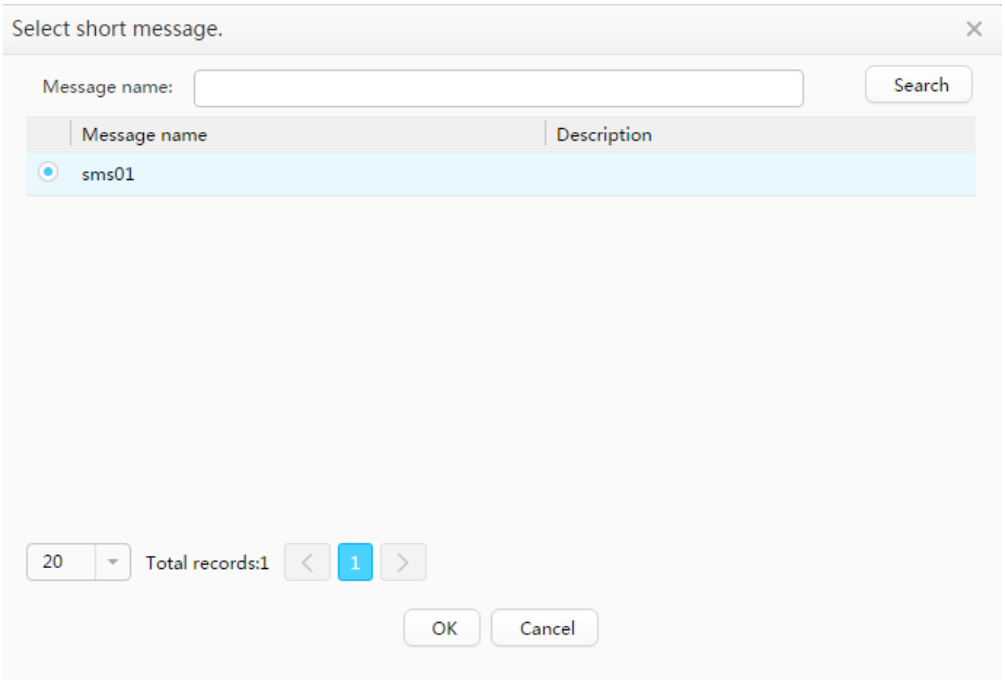


Figure 5-28 Select mobile number



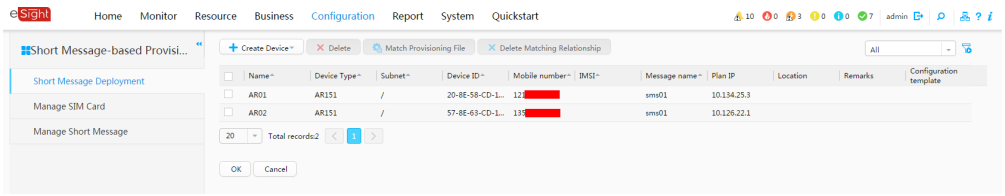
 Copyright © Huawei Technologies Co., Ltd.

Figure 5-29 Select short message



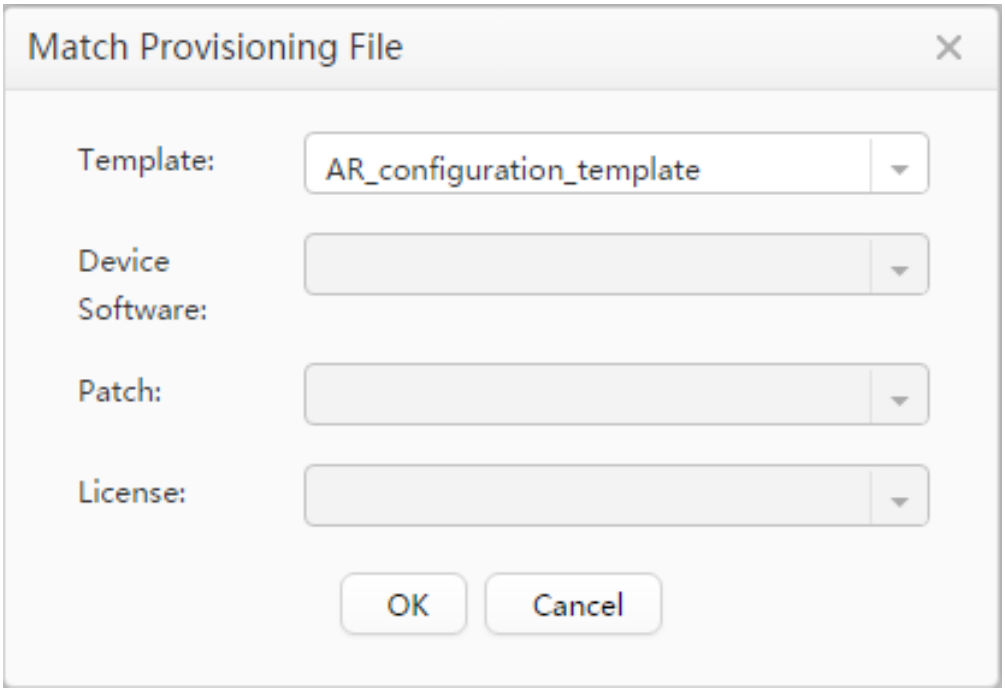
2. Click **OK** to save the configuration, and then the created short messages will be displayed on the **Short Message Deployment** page, as shown in **Figure 5-30**. Select the devices to be deployed and click **Match Provisioning File** to select the created configuration template, as shown in **Figure 5-31**. Click **OK** to save the configuration.

Figure 5-30 Created deployment information



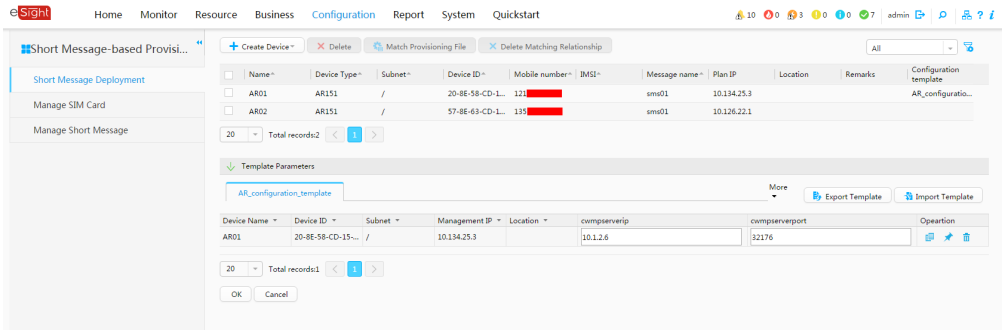
 Copyright © Huawei Technologies Co., Ltd.

Figure 5-31 Matching deployment files



3. After the configuration has been saved, information about the configuration template will be displayed on the **Short Message Deployment** page, as shown in **Figure 5-32**. Click **OK** to finish SMS-based deployment configuration.

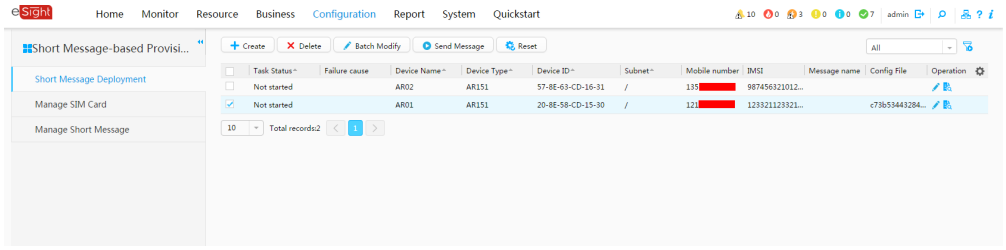
Figure 5-32 SMS-based deployment



4. Select the SMS-based deployment task and click **Send Message** for SMS-based deployment, as shown in **Figure 5-33**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-33 Sending messages



5. View the configuration task status after clicking **Send Message**. Devices receive and parse deployment short messages and connect to eSight in 3G/LTE mode. Devices then obtain file server information and access the file server through SFTP to download and load a configuration file. After loading a configuration file, the devices restart and then register with eSight. You can manage branch devices through eSight after they register successfully.

Step 5 Configure a mobile phone number whitelist.

Configure a mobile phone number whitelist to allow modifying device configurations according to short messages sent from only mobile phone numbers in the whitelist.

```
<Huawei> system-view
[Huawei] sms config caller 456789
Info: Succeed in setting whitelist.
```

Disable SMS-based deployment.

```
[Huawei] undo sms config autodeploy enable
Info: Disable the SMS config function successfully.
```

----End

 Copyright © Huawei Technologies Co., Ltd.

6 Plug-and-Play Deployment Configuration

About This Chapter

This chapter describes how to implement plug-and-play deployment on ARs in the Huawei Cloud Managed Network Solution.

6.1 Overview of Plug-and-Play Deployment

6.2 Understanding Plug-and-Play Deployment

6.3 Application Scenarios for Plug-and-Play Deployment

6.4 Licensing Requirements and Limitations for Plug-and-Play Deployment

6.5 Configuring Plug-and-Play Deployment

6.1 Overview of Plug-and-Play Deployment

Definition

Cloud-based management is a feature in the Huawei Cloud Managed Network Solution. This solution provides a cloud management platform for configuring and maintaining network devices uniformly. In this solution, plug-and-play deployment does not require manual intervention. It is a fast device deployment mode in cloud management scenarios.

Purpose

Traditional network solutions have many network deployment problems, such as high deployment costs and O&M difficulties. These problems are obvious in enterprises with many branches or geographically dispersed branches. Huawei Cloud Managed Network Solution can solve these problems. It implements centralized device management and maintenance through the cloud management platform, significantly reducing network deployment and O&M costs.

 Copyright © Huawei Technologies Co., Ltd.

Plug-and-play deployment implements device deployment without manual intervention on the cloud management platform through the registration center deployed in the Huawei public cloud.

6.2 Understanding Plug-and-Play Deployment

Basic Concepts

- Cloud management platform: is a core component in the Huawei Cloud Managed Network Solution. This component uniformly manages Huawei network devices, such as access routers (ARs), switches, and firewalls. Plug and play of network devices can be implemented through the cloud management platform.
- Registration center: is a main component in the Huawei Cloud Managed Network Solution. This component allows querying device management mode and home cloud management platform. According to the query result, a device determines whether to change to the cloud-based management mode and which cloud management platform it must register with. Currently, ARs work in cloud-based management mode by default.

Process of Implementing Cloud-based Management on ARs

In the Huawei Cloud Managed Network Solution, there are three phases from managed AR deployment to unified device management on the cloud management platform.

1. **ARs obtain the cloud management platform's address information.**

   This phase is the preparation phase in cloud-based management. Routers must first obtain the cloud management platform's URL/IP address and port number. Now these routers are ready to communicate with the cloud management platform. Two methods are available to obtain the cloud management platform's address information, as described in **Table 6-1**.

 Copyright © Huawei Technologies Co., Ltd.

Table 6-1 Methods to obtain the cloud management platform's address information

Method	Description	Scenario	Priority
Through a DHCP server	Option 148 is configured on a DHCP server to carry the cloud management platform's address information. Routers obtain the information through the DHCP server.	This method applies to the cloud managed networks on which devices cannot communicate with the Huawei device registration query center. The cloud management platforms of these networks are often built by enterprises.	High priority. This method is preferred if routers can use multiple methods to obtain the cloud management platform's address information.
Through the registration center	Routers use the Huawei device registration query center's URL/IP address and port number that are preconfigured or obtained through a software upgrade to access the registration center and then obtain the cloud management platform's address information based on their ESNs or MAC addresses.	This method applies to the cloud managed networks on which devices can communicate with the Huawei device registration query center. The cloud management platforms of these networks are the Huawei public cloud platform.	Low priority

2. **ARs register with the cloud management platform for authentication.**

   Routers obtain the cloud management platform's URL/IP address and port number, register with the cloud management platform for authentication, and establish a NETCONF transmission channel. Before the authentication, the cloud management platform needs to import the ESN, device type, and CA certificate of each router. Each router has a local certificate and CA certificate configured before delivery.

3. **ARs are unified managed by the cloud management platform.**

   After NETCONF transmission channels are established, the cloud management platform can manage and operate the routers. All the data exchanged between the cloud management platform and routers will be encrypted.

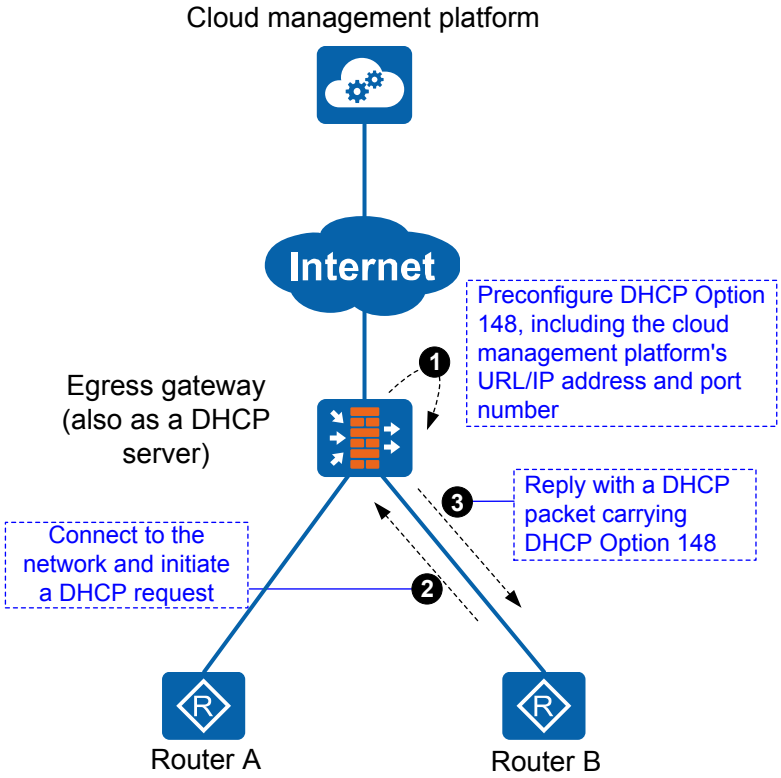
   For details about how the cloud management platform manages routers, see the documentation of the **Huawei Cloud Managed Network Solution**.

 Copyright © Huawei Technologies Co., Ltd.

How to Obtain the Cloud Management Platform's Address Information Through a DHCP Server

In the Huawei Cloud Managed Network Solution, DHCP can implement plug-and-play deployment of routers and configure the cloud management platform's address information. In **Figure 6-1**, administrators need to deploy the DHCP server function on the network egress gateway or deploy an independent DHCP server on the network, and then configure DHCP Option 148, including the cloud management platform's URL/IP address and port number. After a router connects to the network, it initiates a request to the DHCP server to obtain the cloud management platform's address information. After the DHCP server receives the request, it replies with a DHCP packet carrying Option 148. The router receives this DHCP packet, obtains the cloud management platform's URL/IP address and port number, and registers with the cloud management platform for authentication.

Figure 6-1 Obtaining the cloud management platform's address information through a DHCP server

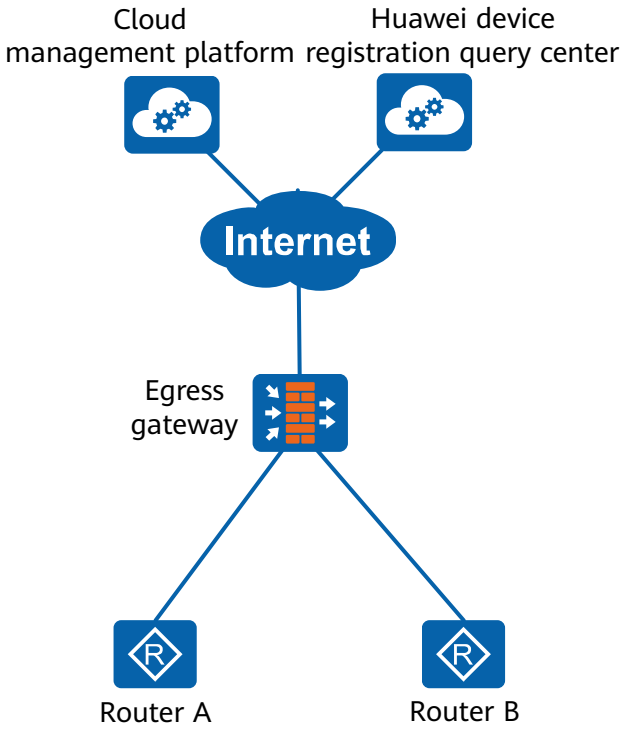


How to Obtain the Cloud Management Platform's Address Information Through the Registration Center

In addition to using DHCP, routers can obtain the cloud management platform's address information through the registration center, implementing plug-and-play deployment. In the network shown in **Figure 6-2**, the cloud management platform needs to establish an HTTP2.0 connection with the registration center and synchronize information about the devices to be managed; routers need to establish an HTTP2.0 connection with the registration center and obtain the cloud management platform's address information.

 Copyright © Huawei Technologies Co., Ltd.

Figure 6-2 Cloud managed network including the registration center

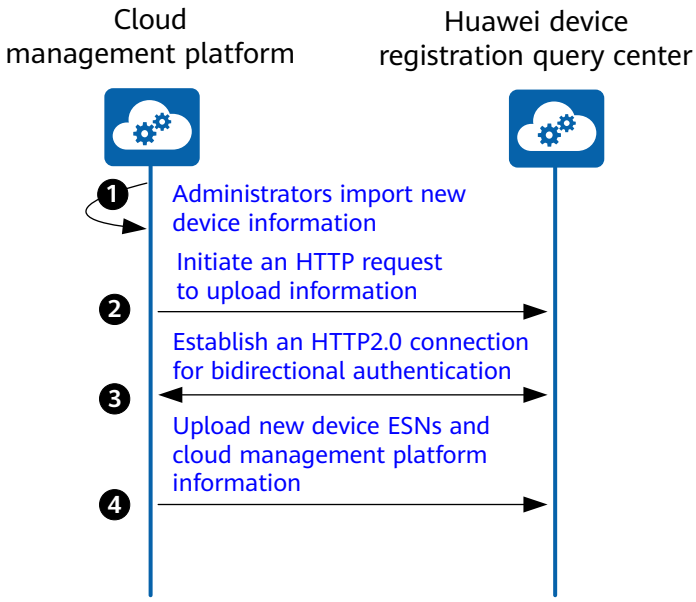


The cloud management platform establishes an HTTP2.0 connection with the registration center.

In **Figure 6-3**, administrators import new device information, including the ESN and device type, into the cloud management platform, and then the cloud management platform initiates an HTTP request to the Huawei device registration query center to upload the information. After the Huawei device registration query center receives the request, it performs bidirectional authentication and establishes an HTTP2.0 connection with the cloud management platform. After the HTTP2.0 connection is established, the cloud management platform uploads the new devices' ESNs and the cloud management platform's address information to the Huawei device registration query center.

 Copyright © Huawei Technologies Co., Ltd.

Figure 6-3 Cloud management platform establishing an HTTP2.0 connection with the registration center

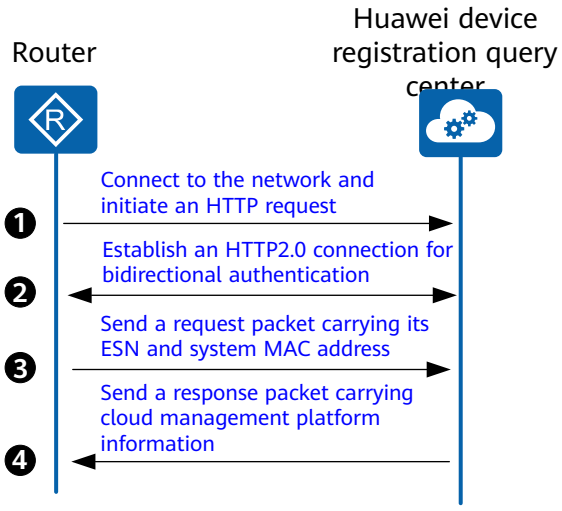


ARs establish an HTTP2.0 connection with the registration center.

The ARs that are delivered most recently and support cloud-based management will have the Huawei device registration query center's URL (register.naas.huawei.com) and port number (10020) preconfigured. The ARs that were delivered earlier and support cloud-based management do not have this URL and port number preconfigured and can be upgraded to the latest software version to obtain default settings. In **Figure 6-4**, after a router connects to the network, it initiates an HTTP request to the registration center. The router and registration center then establish an HTTP2.0 connection for bidirectional authentication. After the connection is established, the router sends a request packet carrying its ESN and system MAC address to the registration center. The registration center receives the request packet, finds the corresponding ESN in the system, and sends a response packet carrying cloud management platform information to the switch. Based on the information, the router can register with the cloud management platform for authentication.

 Copyright © Huawei Technologies Co., Ltd.

Figure 6-4 Routers establishing an HTTP2.0 connection with the registration center



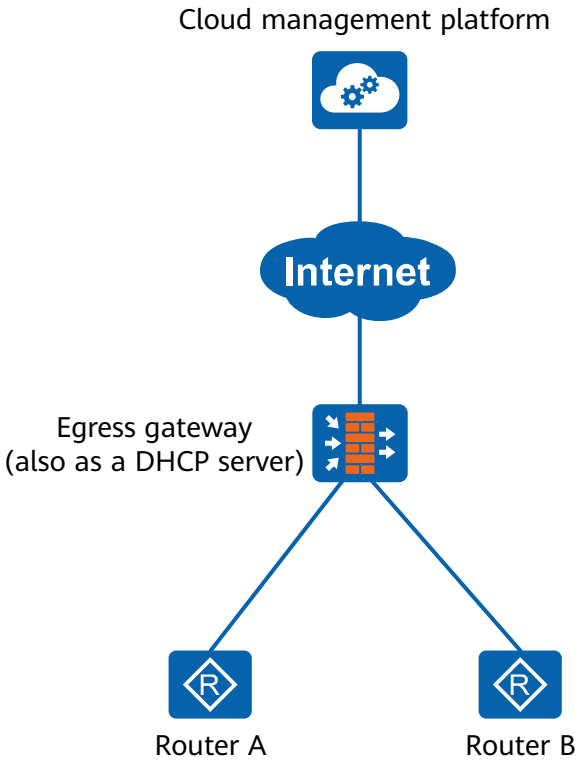
6.3 Application Scenarios for Plug-and-Play Deployment

In the Huawei Agile Cloud Network Solution, routers are plug-and-play and can automatically register with the cloud management platform over the Internet for zero touch deployment. Additionally, cloud-managed routers allow delivering operations through the cloud management platform anytime, anywhere, achieving fast batch service configuration.

In **Figure 6-5**, the egress gateway also functions as the DHCP server, which is configured with Option 148 containing the cloud management platform's address information. Using DHCP, routers obtain the cloud management platform's address information and become plug and play. This networking applies to the enterprise-built cloud management platforms that are not connected to the Huawei device registration query center.

 Copyright © Huawei Technologies Co., Ltd.

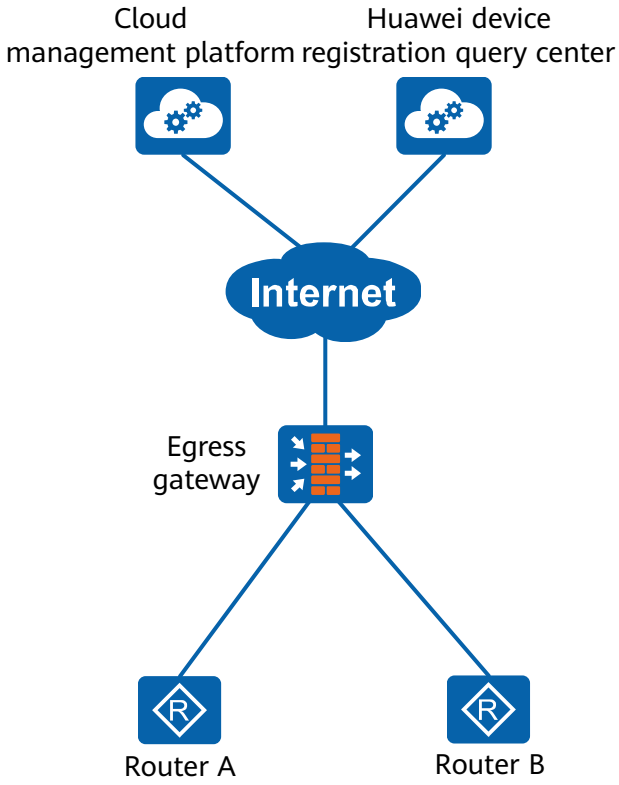
Figure 6-5 Obtaining the cloud management platform's address information through DHCP



In **Figure 6-6**, the Huawei device registration query center is deployed in the cloud managed network solution. The cloud management platform synchronizes the device information imported by administrators to the registration center in real time. Routers then send requests to the registration center, automatically obtain the cloud management platform's address information, and become plug and play. This networking applies to the Huawei public cloud management platform and MSP-built (including enterprise-built) cloud management platforms that are connected to the Huawei device registration query center.

 Copyright © Huawei Technologies Co., Ltd.

Figure 6-6 Obtaining the cloud management platform's address information through the registration center



6.4 Licensing Requirements and Limitations for Plug-and-Play Deployment

Involved Network Elements

In addition to ARs, the cloud managed network solution involves the following network elements:

- Cloud management platform
- Firewalls
- Switches

Licensing Requirements

Plug-and-play deployment is a basic feature of ARs and is not under license control.

Feature Limitations

The plug-and-play function does not take effect when the router cannot meet all the following conditions: unconfigured, no console port input, and no user login.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Only the AR161G-Lc support plug-and-play deployment.

V200R010C10 and later versions support plug-and-play deployment.

6.5 Configuring Plug-and-Play Deployment

Context

In the Huawei Cloud Managed Network Solution, there are three phases from managed AR deployment to unified device management on the cloud management platform.

Procedure

1. ARs obtain the cloud management platform's address information. This phase can be implemented through DHCP and the registration center, as shown in **Table 6-2**.

   Table 6-2 Methods to obtain the cloud management platform's address information

Method	Configuration Procedure
Through a DHCP server	1. Configure option 148 ascii agilemode=tradition;agilemanage-mode=ip;agilemanage-domain=*ip-address*;agilemanage-port=*port-number* on the DHCP server. • **agilemode** indicates the device management mode. • **agilemanage-mode** indicates whether a router obtains the cloud management platform's URL or IP address. • **agilemanage-domain** indicates the cloud management platform's URL or IP address. • **agilemanage-port** indicates the port number used by the cloud management platform. 2. Ensure that the router is unconfigured, has no console port input, and has no user login. After these routers are connected to the network, they automatically obtain the cloud management platform's address information using DHCP.

 Copyright © Huawei Technologies Co., Ltd.

Method	Configuration Procedure
Through the registration center	1. Administrators import device information of routers, including the device ESN and device type, into the cloud management platform. After the information is imported, the cloud management platform uploads the device ESNs and corresponding cloud management platform's address information to the Huawei device registration query center. 2. Ensure that the router is unconfigured, has no console port input, and has no user login routers. The routers that are delivered most recently and support cloud-based management will have the Huawei device registration query center's URL (register.naas.huawei.com) and port number (10020) preconfigured. The routers that were delivered earlier and support cloud-based management do not have this URL (register.naas.huawei.com) and port number (10020) preconfigured and can be upgraded to the latest software version to obtain default settings.

2. ARs register with the cloud management platform for authentication.

   Routers obtain the cloud management platform's URL/IP address, and port number, register with the cloud management platform for authentication, and establish NETCONF transmission channels. Before the authentication, the cloud management platform needs to import the ESN, device type, and CA certificate of each router. Each router has a local certificate and CA certificate configured before delivery.

3. The cloud management platform manages ARs.

   After NETCONF transmission channels are established, the cloud management platform can manage and operate the routers. All the data exchanged between the cloud management platform and routers will be encrypted.

   For details about how the cloud management platform manages routers, see the documentation of the **Huawei Cloud Managed Network Solution**.

 Copyright © Huawei Technologies Co., Ltd.

7 Fast Provisioning Configuration

About This Chapter

The fast provisioning function enables ADSL sub-interfaces, serial sub-interfaces, and Ethernet sub-interfaces on a device to automatically learn configuration information from a peer device.

7.1 Overview of Fast Provisioning
The fast provisioning function enables sub-interfaces on a device to automatically learn configuration information such as the VLAN, IP address, and data link connection identifier (DLCI) from a peer device.

7.2 Enabling the Fast Provisioning Function
After the fast provisioning function is enabled, automatic learning is triggered only when the peer device sends ping packets.

7.3 Maintaining the Fast Provisioning Function
The configuration information learned by a sub-interface can be cleared so that the sub-interface can relearn relevant configurations automatically.

7.4 Licensing Requirements and Limitations for Fast Provisioning
This section provides licensing requirements and limitations for fast provisioning.

7.5 Configuration Examples for Fast Provisioning
This section describes examples for configuring the fast provisioning function, including networking requirements, configuration roadmap, and configuration procedure.

7.1 Overview of Fast Provisioning

The fast provisioning function enables sub-interfaces on a device to automatically learn configuration information such as the VLAN, IP address, and data link connection identifier (DLCI) from a peer device.

When a large number of devices need to be configured in a USB-based deployment scenario, the configuration takes much manpower and time if you need to prepare different configuration files for each device. You can add configuration information about the fast provisioning function in the configuration

 Copyright © Huawei Technologies Co., Ltd.

file used for USB-based deployment. Sub-interfaces on a device to be configured then can automatically learn and save configuration information such as the VLAN, IP address, and DLCI from a peer device.

Fast Provisioning Implementation

Currently, the fast provisioning function is supported by three kinds of sub-interfaces. The implementation processes are different on these sub-interfaces, as described in **Table 7-1**.

Table 7-1 Sub-interfaces supporting the fast provisioning function and the function implementation

Sub-interface	Implementation
ADSL sub-interface: supports the fast provisioning function only when the sub-interface is used in an IPoA scenario and the sub-interface type is P2P.	After the fast provisioning function is enabled on an ADSL sub-interface, the automatic learning function is triggered on the sub-interface when the peer device sends ping packets and the difference between the last byte of the source IP address and that of the destination IP address is one in the ping packets (for example, the source IP address is 192.168.1.1 and the destination IP address is 192.168.1.2). The local device obtains the destination IP address in the ping packets as the IP address of the ADSL sub-interface.

 Copyright © Huawei Technologies Co., Ltd.

Sub-interface	Implementation
Serial sub-interface: supports the fast provisioning function only when the sub-interface is used in a synchronous or asynchronous sub-interface and the sub-interface type is P2P.	After the fast provisioning function is enabled on a serial sub-interface, the device learns the FR Local Management Interface (LMI) protocol type of the peer device. The sub-interface starts automatic learning when the local and peer devices use the same LMI protocol type. The automatic learning function is triggered on the sub-interface when the peer device sends a ping packet and the difference between the source and destination IP addresses in the ping packet is 1. The local device obtains the DLCI from the ping packet and sends the DLCI to a sub-interface capable of automatic learning. The sub-interface then learns the IP address based on the DLCI. **NOTE** If a sub-interface obtains the DLCI but fails to learn the matching IP address, it attempts to learn the IP address again when the peer device sends another ping packet.
Ethernet sub-interface: supports the fast provisioning function only in a scenario where packets carry one VLAN tag.	After the fast provisioning function is enabled on an Ethernet sub-interface, the peer device broadcasts ARP packets in the VLAN before sending ping packets. The automatic learning function of the sub-interface is triggered when the device to be configured finds that the difference between the last byte of the source IP address and that of the destination IP address is one in the ping packets. The sub-interface learns the VLAN information in ARP Request packets and obtains the destination IP address in the packets as the IP address of the sub-interface. **NOTE** If the peer device does not broadcast ARP packets, automatic learning is not triggered on Ethernet sub-interfaces on the local device. The fast provisioning function cannot be enabled simultaneously on two or more sub-interfaces in the same LAN.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- If a sub-interface has been configured with an IP address, the IP address learned automatically by the sub-interface overwrites the original IP address after the fast provisioning function is enabled.
- The fast provisioning function enabled globally and on interfaces will be disabled 1 hour later after the automatic learning function is triggered on a sub-interface. If the device restarts within 1 hour, the fast provisioning function will not be automatically disabled 1 hour later. In this case, the fast provisioning function can only be disabled using the **undo fast provisioning enable** command.
- If the fast provisioning function is enabled on multiple sub-interfaces on a device to be configured, the automatic learning function is triggered on the sub-interfaces in ascending order of sub-interface numbers. For example, the fast provisioning function is enabled on the sub-interfaces GE1/0/0.1 and GE1/0/0.2 of a device. When the **ping 1.1.1.1** and **ping 2.2.2.2** commands are run in sequence on the peer device, GE1/0/0.1 and GE1/0/0.2 automatically learn the IP addresses 1.1.1.1 and 2.2.2.2 respectively.

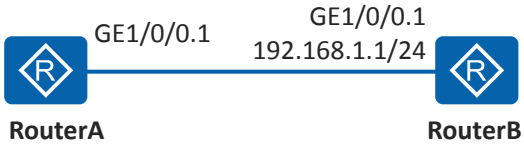
The preceding sub-interfaces learn the mask length according to the ToS value in ping packets. The **Table 7-2** describes the mapping between ToS values and mask lengths.

Table 7-2 Mapping between ToS values and mask lengths

ToS Value	Mask Length
32	31
64	29
96	28
128	27
160	26
192	25
224	24
Other values	30

As shown in **Figure 7-1**, RouterA needs to be configured and is connected to RouterB through VLAN11.

Figure 7-1 Fast provisioning implementation



1. Load the fast provisioning configuration to RouterA using USB-based deployment. Enable the fast provisioning function on GE1/0/0.1 of RouterA.
2. Send ping packets from RouterB. Set the destination IP address of ping packets to 192.168.1.2 and the ToS value to 224. Because the ARP table on

 Copyright © Huawei Technologies Co., Ltd.

RouterB does not contain a MAC address corresponding to 192.168.1.2, RouterB broadcasts ARP Request packets in VLAN11.

3. After receiving ARP Request packets sent by RouterB, RouterA finds that the source IP address is 192.168.1.1 and the destination IP address is 192.168.1.2 in the packets. The automatic learning function is triggered on RouterA. RouterA learns the VLAN information in the ARP Request packets and uses the destination IP address in the packets as the sub-interface IP address. RouterA then sends ARP Reply packets to RouterB. RouterB sends ping packets after it receives the ARP Reply packets. RouterA uses the ToS value in the ping packets to learn the sub-interface mask length. The ToS value in this example is 224 and the mask length is 24 according to **Table 7-2**. GE1/0/0.1 on RouterA automatically learns and saves the following configuration information:

```
#
interface GigabitEthernet1/0/0.1
 dot1q termination vid 11
 ip address 192.168.1.2 255.255.255.0
#
```

7.2 Enabling the Fast Provisioning Function

After the fast provisioning function is enabled, automatic learning is triggered only when the peer device sends ping packets.

Context

When configuring the fast provisioning function, pay attention to the following points:

- After the fast provisioning function is disabled globally using the **undo fast provisioning enable** command, the fast provisioning function configured on interfaces also becomes invalid.
- After enabling the fast provisioning function on an interface, create a sub-interface for the interface. Only the sub-interface can automatically learn information such as the VLAN, IP address, and DLCI from the peer device.
- After the fast provisioning function is enabled, the device starts a timer since the first time the automatic learning function is triggered. The fast provisioning function is automatically disabled globally and on interfaces 1 hour later. If the device restarts within 1 hour, the fast provisioning function will not be automatically disabled 1 hour later. In this case, the fast provisioning function can only be disabled using the **undo fast provisioning enable** command.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **fast provisioning enable** [**restart**] command to enable the fast provisioning function globally.

By default, the fast provisioning function is disabled globally.

Step 3 Enable the fast provisioning function on different sub-interfaces as required.

Configuration on Ethernet interfaces:

 Copyright © Huawei Technologies Co., Ltd.

1. Run the **interface** { **ethernet** | **gigabitethernet** } *interface-number* command to enter the Ethernet interface view.
2. Run the **fast-provisioning enable** command to enable the fast provisioning function on the interface.
3. Run the **quit** command to return to the system view.
4. Run the **interface** { **ethernet** | **gigabitethernet** } *interface-number.subinterface-number* command to create an Ethernet sub-interface and enter the sub-interface view.

Configuration on ADSL interfaces:

1. Run the **interface atm** *interface-number* command to enter the ADSL interface view.
2. Run the **fast-provisioning enable** command to enable the fast provisioning function on the interface.
3. Run the **quit** command to return to the system view.
4. Run the **interface atm** *interface-number.subinterface-number* **p2p** command to create an ADSL sub-interface and enter the sub-interface view.
5. Run the **pvc** *pvc-name vpi/vci* command to create a PVC with specified VPI/VCI and enter the PVC view.
6. Run the **map ip default** command to create an IPoA mapping with a default route for the PVC.
7. Run the **quit** command to return to the ADSL sub-interface view.

Configuration on serial interfaces:

1. Run the **interface serial** *interface-number* command to enter the serial interface view.
2. Run the **link-protocol fr** [**ietf** | **nonstandard**] command to configure the FR encapsulation type for the interface.
3. Run the **fast-provisioning enable** command to enable the fast provisioning function on the interface.
4. Run the **quit** command to return to the system view.
5. Run the **interface serial** *interface-number.subinterface-number* **p2p** command to create serial sub-interfaces and enter the sub-interface view.

   NOTE

   Currently, serial sub-interfaces support the fast provisioning function only when the sub-interface type is P2P.

Step 4 (Optional) Run the **fast-provisioning disable** command to disable the fast provisioning function on sub-interfaces.

----End

Follow-Up Process

Run the **ping** [**-tos** *tos-value*] *host* command on the peer device to trigger automatic learning on the local device.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Automatic learning can only be triggered by using the **ping** *host* or **ping -tos** *tos-value host* command on the peer device.

Verifying the Configuration

- Run the **display fast provisioning state** command to check the status of the fast provisioning function on the interface.
- Run the **display fast provisioning record** [**interface** *interface-type interface-number*] command to check the automatic learning record on an interface enabled with the fast provisioning function.

7.3 Maintaining the Fast Provisioning Function

The configuration information learned by a sub-interface can be cleared so that the sub-interface can relearn relevant configurations automatically.

Context

Configuration information about the fast provisioning function can be automatically loaded to a device to be configured using the USB-based deployment method. After a sub-interface on the device to be configured automatically learns the configuration information, you can clear the configuration information learned by the sub-interface if the configuration information is different from the planned configuration. The sub-interface then can relearn the configuration information.

NOTE

After the fast provisioning function is enabled, the device starts a timer since the first time the automatic learning function is triggered. The fast provisioning function is automatically disabled globally and on interfaces 1 hour later. If the device restarts within 1 hour, the fast provisioning function will not be automatically disabled 1 hour later. In this case, the fast provisioning function can only be disabled using the **undo fast provisioning enable** command.

After a sub-interface finishes automatic learning of configuration information, the automatic learning record is not deleted when configuration on the sub-interface changes. To trigger automatic learning on the sub-interface again, run the **reset fast-provisioning** command on the main interface of the sub-interface to clear configurations on all sub-interfaces of the main interface.

If multiple sub-interfaces of a main interface have finished automatic learning and one of them needs to learn configuration again, run the **reset fast-provisioning** command on the main interface to clear configurations on all the sub-interfaces. The sub-interfaces can then automatically learn the configuration again.

If a new sub-interface is created on a main interface after all the previous sub-interfaces of the main interface finish automatic learning of configurations, run the **reset fast-provisioning** command on the main interface to clear configurations of all the sub-interfaces. Then all the sub-interfaces can automatically learn configurations again.

Procedure

- In the interface view, run the **reset fast-provisioning** command to clear the configuration learned and saved by a specified interface using the fast

 Copyright © Huawei Technologies Co., Ltd.

provisioning function. The sub-interface then can relearn the configuration information.

NOTE

- In the main interface view, run the **reset fast-provisioning** command to clear all the configuration information saved by sub-interfaces of the main interface.
- In the sub-interface view, run the **reset fast-provisioning** command to clear only the IP address saved by the sub-interface.

----End

7.4 Licensing Requirements and Limitations for Fast Provisioning

This section provides licensing requirements and limitations for fast provisioning.

Involved Network Elements

None

Licensing Requirements

Configuring the fast provisioning is a basic feature of a router and is not under license control.

Feature Limitations

None

7.5 Configuration Examples for Fast Provisioning

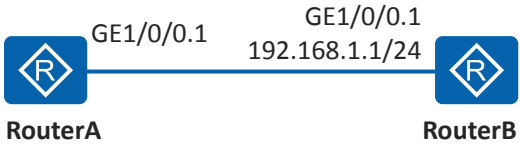
This section describes examples for configuring the fast provisioning function, including networking requirements, configuration roadmap, and configuration procedure.

7.5.1 Example for Configuring the Fast Provisioning Function

Networking Requirements

As shown in **Figure 7-2**, RouterA and RouterB are connected through VLAN11. It is required that GE1/0/0.1 on RouterA should automatically learn VLAN and IP address settings.

Figure 7-2 Networking diagram for configuring the fast provisioning function



 Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

The configuration roadmap is as follows:

1. Make a configuration file and load the file to RouterA using the USB-based deployment method so that the fast provisioning function is enabled on RouterA without manual configuration.
2. Configure basic information about a sub-interface on RouterB and send ping packets to trigger the automatic learning function on GE1/0/0.1 of RouterA. GE1/0/0.1 then can automatically learn VLAN and IP address settings.

Procedure

Step 1 Make a configuration file that contains configuration information about the fast provisioning function. The process of making the file is not provided here. The fast provisioning configuration information is as follows:

```
#
 fast provisioning enable
#
interface GigabitEthernet1/0/0
 fast-provisioning enable
#
interface GigabitEthernet1/0/0.1
#
```

Step 2 Perform USB-based deployment on RouterA. Load the configuration file to RouterA using the USB-based deployment method. For the detailed USB-based deployment process, see **4.6.1 Example for Configuring USB-based Deployment**.

After USB-based deployment is performed on RouterA successfully, view the automatic learning record of the interface enabled with the fast provisioning function on RouterA.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] display fast provisioning state
----------Fast Provisioning State----------
GigabitEthernet1/0/0
   GigabitEthernet1/0/0.1
      State : enable
-------------------------------------------
```

Step 3 Configure a sub-interface on RouterB.

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface gigabitethernet 1/0/0.1
[RouterB-GigabitEthernet1/0/0.1] dot1q termination vid 11
[RouterB-GigabitEthernet1/0/0.1] ip address 192.168.1.1 255.255.255.0
[RouterB-GigabitEthernet1/0/0.1] quit
```

Step 4 Send ping packets from RouterB to trigger the automatic learning function on RouterA. Set the destination IP address of ping packets to 192.168.1.2 and the ToS value to 224.

```
[RouterB] ping -tos 224 192.168.1.2
 PING 192.168.1.2 : 56  data bytes, press CTRL_C to break
   Request time out
   Reply from 192.168.1.2 : bytes=56 Sequence=2 ttl=255 time=4 ms
   Reply from 192.168.1.2 : bytes=56 Sequence=3 ttl=255 time=530 ms
   Reply from 192.168.1.2 : bytes=56 Sequence=4 ttl=255 time=4 ms
   Reply from 192.168.1.2 : bytes=56 Sequence=5 ttl=255 time=1 ms

 --- 192.168.1.2  ping statistics ---
```

 Copyright © Huawei Technologies Co., Ltd.

```
  5 packet(s) transmitted
  4 packet(s) received
  20.00% packet loss
  round-trip min/avg/max = 1/134/530 ms
```

Step 5 Verify the configuration.

View the automatic learning record of GE1/0/0.1 enabled with the fast provisioning function on RouterA.

```
[RouterA] display fast provisioning record
----------Fast Provisioning Record----------
GigabitEthernet1/0/0.1
  State : successful
  Vlan : 11
  IP : 192.168.1.2        Mask :24
Fast provisioning num : 1
------------------------------------------------
```

The preceding command output shows that GE1/0/0.1 on RouterA learns the VLAN tag value 11, IP address 192.168.1.2, and mask length 24.

View the saved configuration information of GE1/0/0.1 on RouterA.

```
[RouterA] interface gigabitethernet 1/0/0.1
[RouterA-GigabitEthernet1/0/0.1] display this
[V200R005C10]
#
interface GigabitEthernet1/0/0.1
 dot1q termination vid 11
 ip address 192.168.1.2 255.255.255.0
#
return
```

The preceding command output shows that configuration information such as the IP address learned by GE1/0/0.1 on RouterA is saved.

----End

Configuration File

Configuration file of RouterB

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0.1
 dot1q termination vid 11
 ip address 192.168.1.1 255.255.255.0
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

8 First Login to a Device

About This Chapter

To enter the CLI of a new device to perform basic configuration, you must log in to the device for the first time through a console port or mini USB port.

8.1 Overview of the First Login

8.2 Licensing Requirements and Limitations for the First Login
This section provides the licensing requirements and limitations for logging in to a device for the first time.

8.3 Logging In to a Device

8.4 Basic Configuration on a Device at the First Login (Console Port or Mini USB Port)

8.5 Configuration Examples for Logging In to a Device for the First Time

8.1 Overview of the First Login

This section describes login modes supported by the device when you log in for the first time and the corresponding basic configuration.

To configure a new device, log in to the device first. A device supports first login through the console port or the mini USB port.

The main control unit of a device provides a console port and a mini USB port. To configure a device, connect the user terminal serial port to the device console port or connect the user terminal USB port to the mini USB port of the device.

After login, configure the system time, device name, management IP address, and user level and authentication mode for Telnet users to facilitate subsequent configuration.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- Before logging in to the device using the mini USB port, install the mini USB port driver on the user terminal.

  To obtain the mini USB driver, visit **https://support.huawei.com/enterprise** and select **AR_MiniUSB_driver** to download. The mini USB driver supports only Windows XP, Windows Vista, and Windows 7 operating systems.
- When both the mini USB port and console port are connected to the user terminal, only the mini USB port can be used for login.

8.2 Licensing Requirements and Limitations for the First Login

This section provides the licensing requirements and limitations for logging in to a device for the first time.

Involved Network Elements

None

Licensing Requirements

Logging in to a device for the first time is a basic feature of a router and is not under license control.

Feature Limitations

None

8.3 Logging In to a Device

8.3.1 Logging In to a Device for the First Time Through a Console Port

You can log in to a device that is being powered on for the first time through a console port from a PC. After that, you can perform basic configuration on the device and manage the device.

Pre-configuration Tasks

Before logging in to the device through the console port, complete the following tasks:

- Power on the device properly.
- Prepare the console cable (delivered with AR2204E-D&AR2204E-D-27GE&AR2220E&AR2240&AR2240C&AR3200&AR3600 series)
- Install the terminal emulation software on the PC.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

You can use the self-contained terminal emulation software of the operating system (such as PuTTY) on your PC. If the operating system does not provide terminal emulation software, use third-party terminal emulation software. For details, see the software user guide or online help.

Default Settings

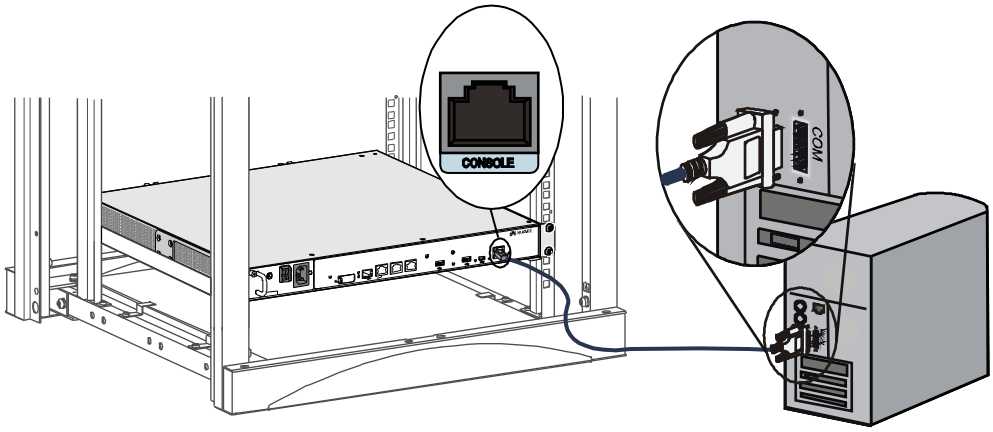
Table 8-1 Default settings for the console port

Parameter	Default Setting
Baud rate	9600 bit/s
Flow control	None
Parity	None
Stop bits	1
Data bits	8

Procedure

Step 1 Connect the DB9 female connector of the console cable to the COM port on the PC, and connect the RJ45 connector to the console port on the device, as shown in Figure 8-1.

Figure 8-1 Connecting to the device through the console port

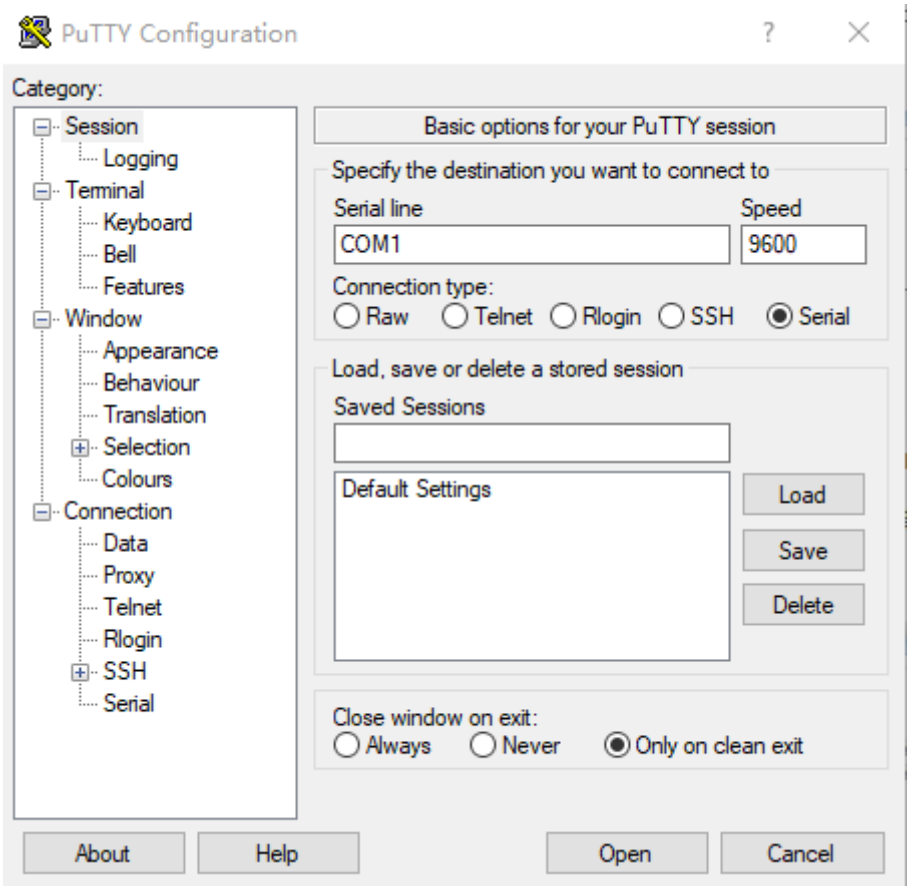


Step 2 Start the terminal emulation software on the PC. Create a connection, select the connected port, and set communication parameters. (This section uses the third-party software PuTTY as an example.)

1. Click  to establish a connection, as shown in Figure 8-2.

 Copyright © Huawei Technologies Co., Ltd.

Figure 8-2 Establishing a connection



2. Set the connected port and communication parameters, as shown in **Figure 8-3**.

   Select the connected port based on actual situations. For example, you can view port information in **Device Manager** in the Windows operating system, and select the connected port.

   Communication parameters of the terminal emulation software must be consistent with the default attribute settings of the console user interface on the device, which are 9600 bit/s baud rate, 8 data bits, 1 stop bit, no parity check, and no flow control.

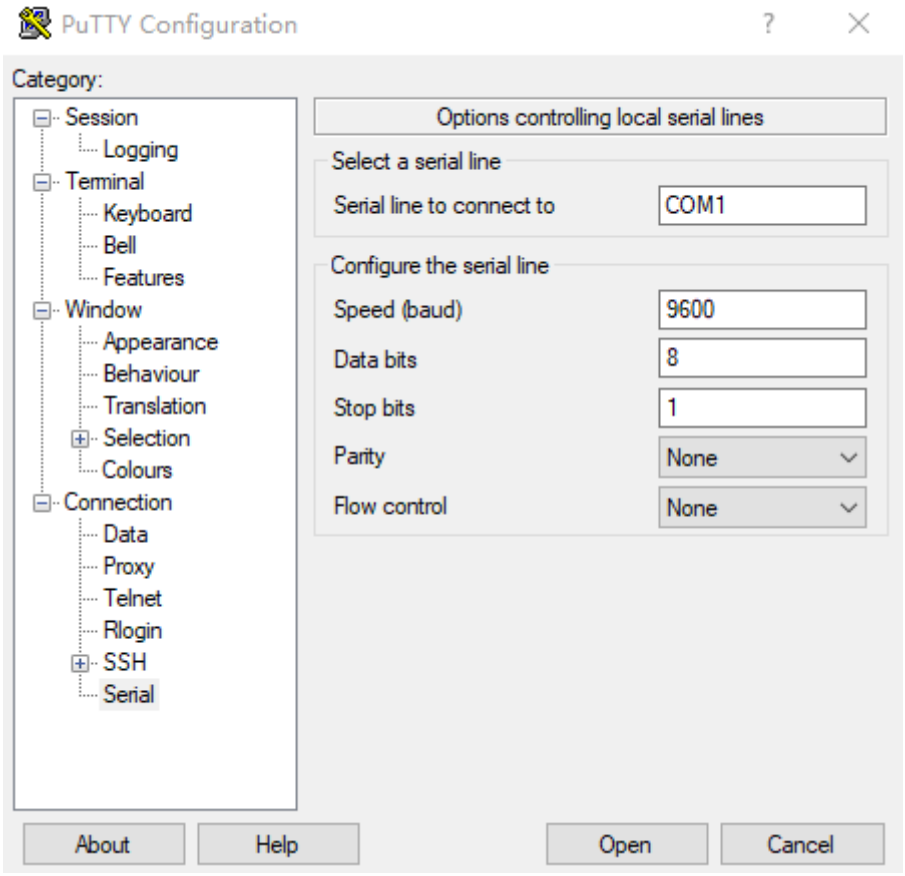
   NOTE

   By default, no flow control mode is configured on the device. Because RTS/CTS is selected in the software by default, you need to deselect RTS/CTS; otherwise, you cannot enter commands.

   If you modify the serial port communication parameters on the device, you must make the same modifications on the PC and then create a connection again.

 Copyright © Huawei Technologies Co., Ltd.

Figure 8-3 Setting the connected port and communication parameters



Step 3 Click **Connect**. The following information is displayed. Enter the password. The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

```
Login authentication

Username:admin
Password:
<Huawei>
Info: The entered password is the same as the default. You are advised to change
 it to ensure security.
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- The password entered in interactive mode is not displayed on the screen.
- You are advised to change the password after login and update the password regularly to ensure security.
- If the configuration file contains a plain-text password or the entered password is an encryption password with low security, the system displays the message "There are security risks in the configuration file. You are advised to save the configuration immediately. If you choose to save, the current configuration file will be unavailable after version downgrade. Are you sure to save now?[y/n]:" when you log in to the device.
  - If you need to save the current configuration, enter **y** and press **Enter**.
  - If you do not need to save the current configuration, enter **n** and press **Enter**. It is recommended that you enter **y**.
- When you connect to a new or unconfigured device through a console port, the following information is displayed:

  Auto-Config is working. Before configuring the device, stop Auto-Config. If you perform configurations when Auto-Config is running, the DHCP, routing, DNS, and VTY configurations will be lost. Do you want to stop Auto-Config? [y/n]:
  - To continue Auto-Config, enter **n** and press **Enter**.
  - To stop Auto-Config, enter **y** and press **Enter**.

You can run commands to configure the device. Enter a question mark (?) whenever you need help.

----End

8.3.2 Logging In to a Device for the First Time Through a Mini USB Port

If no console port is available on your PC, you can use a mini USB cable to connect a USB port on the PC to the mini USB port of a device that is being powered on for the first time. After that, you can perform basic configuration on the device and manage the device.

Pre-configuration Tasks

Before logging in to a device through the mini USB port, complete the following tasks:

- Power on the device.
- Prepare a mini USB cable. (You can use type-B mini USB cable, which is not delivered with the device.)
- OObtain the mini USB driver that is compatible with the PC's operating system. Install the mini USB driver on the PC.

  NOTE

  To obtain the mini USB driver, visit **https://support.huawei.com/enterprise** and select **AR_MiniUSB_driver** to download. The mini USB driver supports only Windows XP, Windows Vista, and Windows 7 operating systems.
- Installing the terminal emulation software on the PC

 Copyright © Huawei Technologies Co., Ltd.

NOTE

You can use the self-contained terminal emulation software of the operating system (such as the PuTTY) on the PC. If no built-in terminal emulation software is available, use the third-party terminal emulation software. For details, see the software user guide or online help.

Default Settings

Table 8-2 Default settings for the mini USB port

Parameter	Default Setting
Baud rate	9600 bit/s
Flow control	None
Parity	None
Stop bits	1
Data bits	8

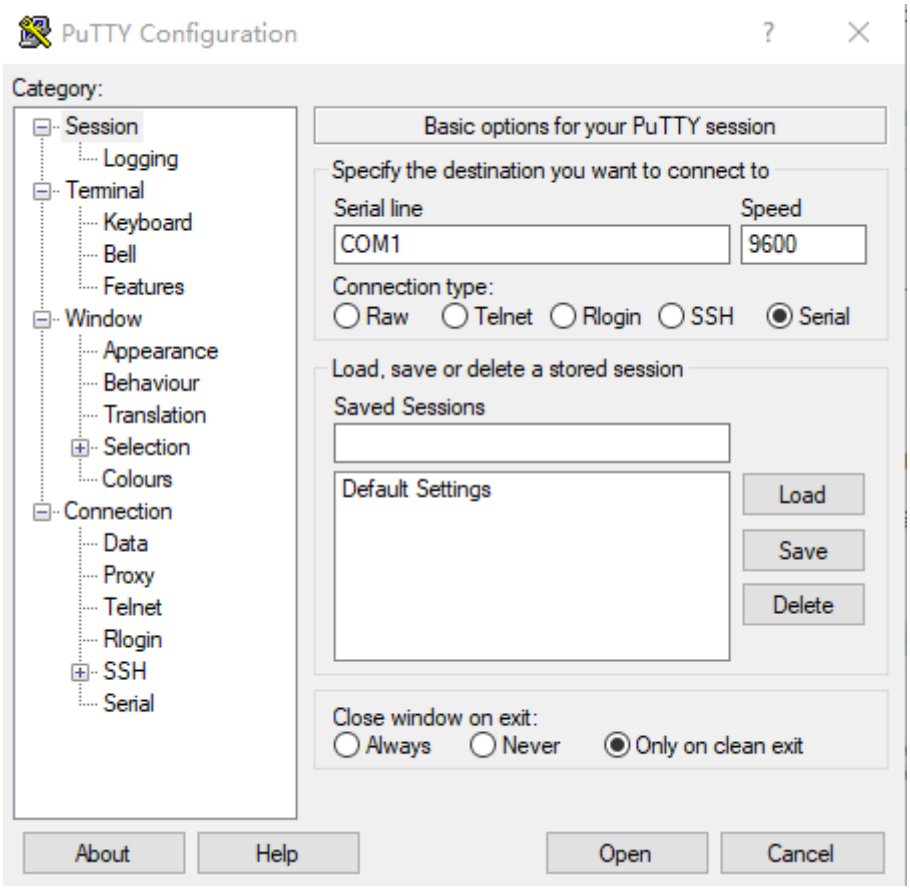
Procedure

Step 1 Start the terminal emulation software on the PC. Create a connection, select the connected port, and set communication parameters. (This section uses the third-party software PuTTY as an example.)

1. Click  to establish a connection, as shown in **Figure 8-4**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 8-4 Establishing a connection



2. Set the connected port and communication parameters, as shown in **Figure 8-5**.

   Select the connected port based on actual situations. For example, you can view port information in **Device Manager** in the Windows operating system, and select the connected port.

   Communication parameters of the terminal emulation software must be consistent with the default attribute settings of the console user interface on the device, which are 9600 bit/s baud rate, 8 data bits, 1 stop bit, no parity check, and no flow control.

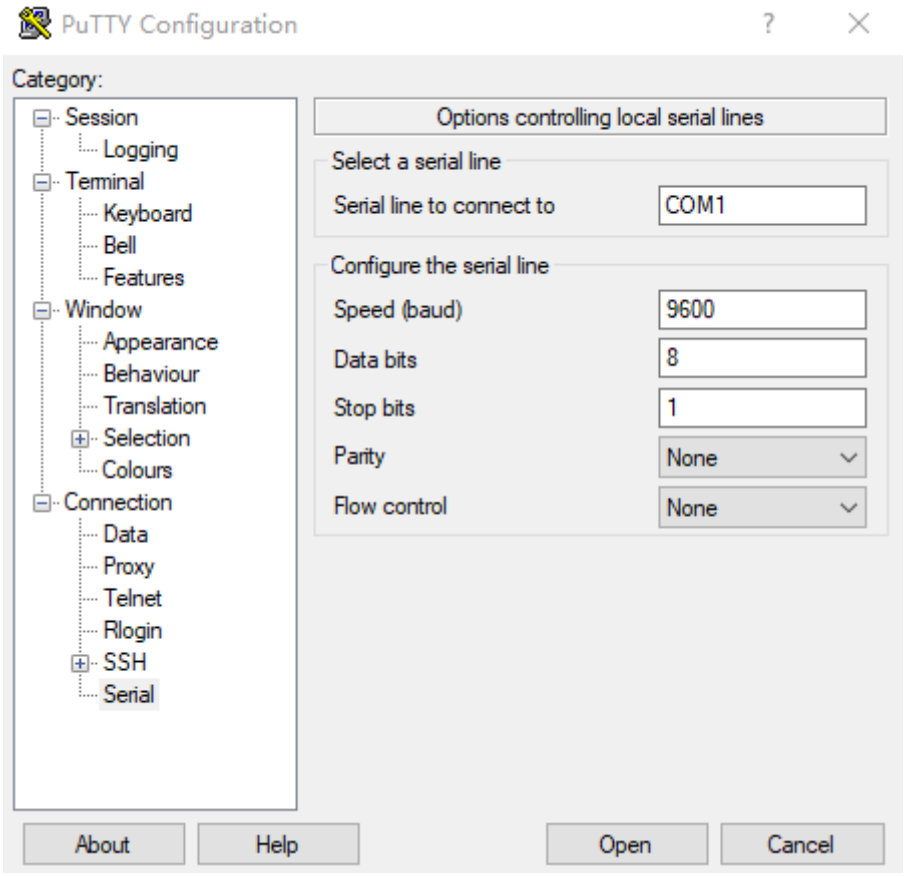
   NOTE

   By default, no flow control mode is configured on the device. Because RTS/CTS is selected in the software by default, you need to deselect RTS/CTS; otherwise, you cannot enter commands.

   If you modify the serial port communication parameters on the device, you must make the same modifications on the PC and then create a connection again.

 Copyright © Huawei Technologies Co., Ltd.

Figure 8-5 Setting the connected port and communication parameters



Step 2 Click **Connect**. The following information is displayed. Enter the password. The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

```
Login authentication

Username:admin
Password:
<Huawei>
Info: The entered password is the same as the default. You are advised to change
 it to ensure security.
```

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- The password entered in interactive mode is not displayed on the screen.
- You are advised to change the password after login and update the password regularly to ensure security.
- If the configuration file contains a plain-text password or the entered password is an encryption password with low security, the system displays the message "There are security risks in the configuration file. You are advised to save the configuration immediately. If you choose to save, the current configuration file will be unavailable after version downgrade. Are you sure to save now?[y/n]:" when you log in to the device.
  - If you need to save the current configuration, enter **y** and press **Enter**.
  - If you do not need to save the current configuration, enter **n** and press **Enter**. It is recommended that you enter **y**.
- When you connect to a new or unconfigured device through a console port, the following information is displayed:

  Auto-Config is working. Before configuring the device, stop Auto-Config. If you perform configurations when Auto-Config is running, the DHCP, routing, DNS, and VTY configurations will be lost. Do you want to stop Auto-Config? [y/n]:
  - To continue Auto-Config, enter **n** and press **Enter**.
  - To stop Auto-Config, enter **y** and press **Enter**.

You can run commands to configure the device. Enter a question mark (?) whenever you need help.

----End

8.4 Basic Configuration on a Device at the First Login (Console Port or Mini USB Port)

Context

This section describes how to configure the time and date, character set in the system, device name, management IP address, and the user level and authentication mode for Telnet users at first login through the console port or mini USB port.

Procedure

Step 1 Set the time and date on the device.

1. Run **clock timezone** *time-zone-name* { **add** | **minus** } *offset*

   The time zone is set.

   If you do not specify the time zone name, the system uses **Default Zone Name**.

   - **add**: adds the specified time zone offset to the Coordinated Universal Time (UTC). That is, the sum of the default UTC time zone and *offset* equals the time zone specified by *time-zone-name*.
   - **minus**: subtracts the specified time zone offset from the UTC. That is, the remainder obtained by subtracting *offset* from the default UTC time zone equals the time zone specified by *time-zone-name*.

 Copyright © Huawei Technologies Co., Ltd.

2. Run **clock datetime** *HH:MM:SS YYYY-MM-DD*

   The current time and date are set.

   If the time zone is not set, the time set using this command is considered as the UTC time. Before setting the current time, you are advised to confirm the current zone and set the correct time zone offset.

3. (Optional) Run **clock daylight-saving-time** *time-zone-name* **one-year** *start-time start-date end-time end-date offset***clock daylight-saving-time** *time-zone-name* **repeating** *start-time* { { **first** | **second** | **third** | **fourth** | **last** } *weekday month* | *start-date1* } *end-time* { { **first** | **second** | **third** | **fourth** | **last** } *weekday month* | *end-date1* } *offset* [*start-year* [*end-year*]]

   Or

   Daylight saving time (DST) is set.

   By default, DST is not configured.

   If you configure periodic DST, the combination of the DST start time and end time can be any of the following: date+date, day of the week+day of the week, date+day of the week, and day of the week+date. For the configuration method, see **clock daylight-saving-time**.

   When DST is used, you can run the **clock timezone** *time-zone-name* { **add** | **minus** } *offset* command to set the time zone. The time zone in the output of the **display clock** command is, however, the name of the DST time zone. When DST ends, the system displays the original time zone.

Step 2 (Optional) Configure the character set in the system.

NOTE

You can configure the character set so that the system supports only English input or both Chinese and English inputs.

1. Run **system-view**

   The system view is displayed.

2. Run **language character-set** *character*

   The character set in the system is configured.

   The default character set in the system is ISO8859-1, that is, the system supports only English input.

3. Run **quit**

   Exit from the system view.

Step 3 (Optional) Enables the password authentication function for users who enter the diagnostic view.

1. Run **system-view**

   The system view is displayed.

2. Run **diagnose verify enable**

   Enables the password authentication function for users who enter the diagnostic view.

 Copyright © Huawei Technologies Co., Ltd.

By default, password authentication is not required for users who enter the diagnostic view.

3. Run **quit**

   Exit from the system view.

Step 4 (Optional) Enables the query response processing function for the NETBIOS name service and specifies the type and number of the response interface.

1. Run **system-view**

   The system view is displayed.

2. Run **interface** *interface-type interface-number*

   The interface view is displayed.

3. Run **ip address** *ip-address* { *mask* | *mask-length* }

   The management IP address is assigned.

4. Run **dhcp select interface**

   Enables an interface to use the interface address pool.

5. Run **quit**

   Return to the interface view.

6. Run **ip address** *ip-address* { *mask* | *mask-length* }

   Configure the IP under the query response interface.

7. Run **quit**

   Return to the system view.

8. Run **ip netbios-reply interface**

   Enables the query response processing function for the NETBIOS name service and specifies the type and number of the response interface.

Step 5 Set the device name and management IP address.

1. Run **system-view**

   The system view is displayed.

   By default, the query response processing function for the NETBIOS name service is disabled.

2. Run **sysname** *host-name*

   The device name is set.

   By default, the device name is Huawei.

3. Run **interface** *interface-type interface-number*

   The interface view is displayed.

   In addition to the management interface on the device, you can also assign the management IP address to Layer 3 interfaces such as VLANIF interfaces on the device.

4. Run **ip address** *ip-address* { *mask* | *mask-length* }

   The management IP address is assigned.

 Copyright © Huawei Technologies Co., Ltd.

The management IP address is used to maintain and manage the device. Configure the IP address and routes based on the network plan to ensure that the routes between the terminal and device are reachable.

5. Run **quit**

   Return to the system view.

Step 6 Set the user level and authentication mode for Telnet users.

1. Run **telnet** [**ipv6**] **server enable**

   The Telnet server is enabled.

   By default, the Telnet server is disabled.

2. Run **user-interface vty** *first-ui-number* [*last-ui-number*]

   The VTY user interface view is displayed.

3. Run **protocol inbound** { **all** | **telnet** }

   The VTY user interface is configured to support the Telnet protocol.

   By default, a VTY user interface supports the SSH and Telnet protocol.

4. Run **user privilege level** *level*

   The Telnet user level is set.

   By default, users who log in through the VTY user interface can access commands at level 0.

5. Run **authentication-mode aaa**

   The authentication mode for Telnet users is set to AAA authentication.

   By default, no authentication mode is configured for the VTY user interface. For the users logging in to the VTY interface, an authentication method must be configured; otherwise, users cannot log in.

   NOTE

   The system provides two authentication modes: AAA authentication and password authentication. AAA authentication requires both the user name and password, which is more secure than password authentication. This section describes how to configure AAA authentication. For the configuration method of other authentication modes, see **Configuring an Authentication Mode for a VTY User Interface**.

6. Run **aaa**

   The AAA view is displayed.

7. Run **local-user** *user-name* **password irreversible-cipher** *password*

   The user name and password for login through Telnet are configured.

   The value of *password* can be a plain-text string of 8 to 128 characters or a cipher-text string of 68 characters.

   A too simple password may cause a potential security risk. To enhance the security strength, the password entered in plain text must contain at least two of the following: uppercase letters, lowercase letters, digits, and special characters, and special characters except the question mark (?). In addition, the password cannot be the same as the user name or the mirror user name.

 Copyright © Huawei Technologies Co., Ltd.

8. Run **local-user** *user-name* **service-type telnet**

   The login mode is set to Telnet.

Step 7 Save the configuration.

After basic configuration is complete, you are advised to save the configuration. If the configuration is lost, the connection and configuration for the first login must be performed again.

1. Run **return**

   Return to the user view.
2. Run **save**

   The configuration is saved.

   The current configuration has been saved in the configuration file. For details, see **12.3.1 Saving the Configuration File**.

----End

Verifying the Configuration

- Run the **display clock** command to check the current date and clock setting.
- Run the **display ip interface brief** [*interface-type* [*interface-number*]] command to check brief information about the IP address on the interface.
- Run the **display user-interface** [*ui-type ui-number1* | *ui-number*] [**summary**] command to check the physical attributes and configuration of the user interface.
- Run the **display local-user** command to check the local user list.

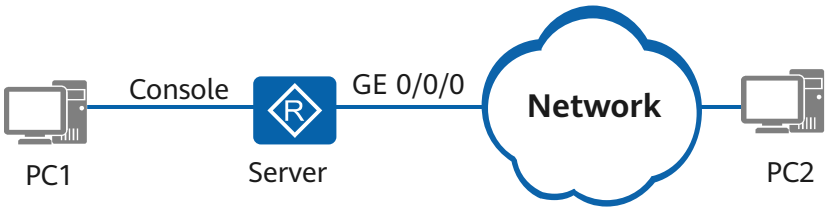
8.5 Configuration Examples for Logging In to a Device for the First Time

8.5.1 Example for Performing Basic Configuration on the Device at First Login

Networking Requirements

After logging in to the device through the console port, perform basic device configuration, and set the user level to 15 and authentication mode to AAA for users 0-4 who perform remote login through Telnet.

Figure 8-6 Networking diagram for configuring the device through the console port



 Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

1. Log in to the device through the console port.
2. Configure the device.

Procedure

Step 1 Log in to the device from PC1 through the console port. For details, see **Logging In to a Device for the First Time Through a Console Port**.

Step 2 Configure the device.

Set the system date, time, and time zone.

```
<Huawei> clock timezone BJ add 08:00:00
<Huawei> clock datetime 20:10:00 2015-03-26
```

Set the device name and IP address of the management interface.

```
<Huawei> system-view
[Huawei] sysname Server
[Server] interface gigabitethernet 0/0/0
[Server-GigabitEthernet0/0/0] ip address 10.137.217.177 24
[Server-GigabitEthernet0/0/0] quit
```

Set the user level and authentication mode for Telnet users.

```
[Server] telnet server enable
[Server] user-interface vty 0 4
[Server-ui-vty0-4] user privilege level 15
[Server-ui-vty0-4] authentication-mode aaa
[Server-ui-vty0-4] quit
[Server] aaa
[Server-aaa] local-user admin1234 password irreversible-cipher Helloworld@6789
[Server-aaa] local-user admin1234 privilege level 15
[Server-aaa] local-user admin1234 service-type telnet
[Server-aaa] quit
```

Step 3 Verify the configuration.

When completing the configuration, you can log in to the device through Telnet on PC2.

Access the command line interface of Windows operating system and log in to the device through Telnet.

```
C:\Documents and Settings\Administrator> telnet 10.137.217.177
```

Press **Enter**. On the displayed login page, enter the user name and password. If the authentication succeeds, the command line interface for the user view is displayed. (The following information is only for reference.)

```
Username:admin1234
Password:
<Server>
```

----End

Configuration Files

```
#
 sysname Server
```

 Copyright © Huawei Technologies Co., Ltd.

```
#
 clock timezone BJ add 08:00:00
#
aaa
 local-user admin1234 password irreversible-cipher %^%#*~Br";[g6Pv5Zf>$~{hY+N!`{$<[Y{;l02P)B,EBz\1FN!c
+%^%#
 local-user admin1234 privilege level 15
 local-user admin1234 service-type telnet
#
interface GigabitEthernet0/0/0
 ip address 10.137.217.177 255.255.255.0
#
 telnet server enable
#
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 15
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

9 CLI Login Configuration

About This Chapter

You can log in to a device through its console port or mini USB port, or using Telnet, redirection, reverse Telnet, or STelnet to manage and maintain the device.

9.1 Overview of CLI Login Methods
You can log in to a device through its console port or mini USB port, or using Telnet or STelnet. After successful login, you can run commands on the command line interface (CLI) to manage and configure the device. You can also log in to another device from the local device using Telnet, STelnet, redirection, or reverse Telnet.

9.2 Overview of User Interfaces
The system supports console, TTY, and VTY user interfaces.

9.3 Licensing Requirements and Limitations for CLI Login
This section provides licensing requirements and limitations for CLI login.

9.4 Configuring Login Through a Console Port
You can connect a PC to the console port of a device and then log in to the device to perform basic configurations and management.

9.5 Configuring Login Through the Mini USB Port
You can connect a PC to the mini USB port of a device and then log in to the device to perform basic configurations and management.

9.6 Configuring Telnet Login
You can log in to a device using Telnet to manage and configure the device.

9.7 Configuring STelnet Login
You can log in to a device using STelnet to manage and configure the device.

9.8 Configuring the Redirection Function for Device Login
After completing redirection configuration, you can log in to a remote serial port device from the local device to configure and manage the remote device.

9.9 Configuring Reverse Telnet Login

 Copyright © Huawei Technologies Co., Ltd.

The reverse Telnet function enables dumb terminals that are directly connected to a router using asynchronous serial cables or console cables to log in to a remote server.

9.10 Typical Operations After Login
After logging in to a device through a console port or mini USB port, or using Telnet or STelnet, you can perform service configurations and the following common operations on the device.

9.11 Configuration Examples for CLI Login
This section describes examples of logging in to a device through a console port, Telnet, or STelnet.

9.12 Troubleshooting CLI Login
This section describes common faults caused by incorrect configurations and provides the corresponding troubleshooting procedures.

9.13 FAQ About CLI Login
This section describes common problems you may encounter during the configuration and provides the solutions to these problems.

9.1 Overview of CLI Login Methods

You can log in to a device through its console port or mini USB port, or using Telnet or STelnet. After successful login, you can run commands on the command line interface (CLI) to manage and configure the device. You can also log in to another device from the local device using Telnet, STelnet, redirection, or reverse Telnet.

You can log in to a device using one of the CLI methods described in **Table 9-1** to configure and manage the device.

 Copyright © Huawei Technologies Co., Ltd.

Table 9-1 CLI login methods

Login Method	Advantages	Disadvantages	Applicable Scenario	Description
Logging In Through the Console Port	A dedicated console cable is used for effective device control.	You cannot remotely log in to a device to maintain it.	• When you need to configure a device that is powered on for the first time, log in to the device through the console port. • If you cannot remotely log in to a device, you can log in through the console port. • If a device fails to start, you can enter the BootROM menu through the console port to diagnose the fault or upgrade the device.	Console port login is the basis for other login methods. By default, you can log in to a device through a console port and has the user level of 15 after login.
Logging In Through the Mini USB Port	If no console port is available on a PC, you can use a mini USB cable to connect the USB port on the PC to the mini USB port of a device and then log in to the device for effective control.	You cannot remotely log in to a device to maintain it.	When you need to configure a device that is powered on for the first time but no console port is available on your PC, log in to the device through the mini USB port.	The device connection for mini USB port login is different from that for console port login but the configurations are the same after login.

 Copyright © Huawei Technologies Co., Ltd.

Login Method	Advantages	Disadvantages	Applicable Scenario	Description
Logging In Through Telnet	You can log in to one device using Telnet to remotely manage and maintain several devices without the need to connect each device to a terminal, which facilitates operations.	Data is transmitted using TCP in plain text, which is a potential security risk.	If you need to configure a device remotely, log in to the device using Telnet. Telnet login is typically used with networks that do not require high security.	By default, you cannot log in to a device directly using Telnet. Before using Telnet to log in, you must locally log in to the device through a console port or mini USB port, and perform the following configurations: • Configure a reachable route between the user terminal and device. (By default, no management IP address is configured on the device.) • Enable the Telnet server function and set parameters. • Configure a user interface for Telnet login.

 Copyright © Huawei Technologies Co., Ltd.

Login Method	Advantages	Disadvantages	Applicable Scenario	Description
Logging In Through STelnet	The Secure Shell (SSH) protocol provides secure remote logins on insecure networks to ensure data integrity and reliability, and secure data transmission.	The configuration is complex.	You can log in to a device using STelnet on networks with high security requirements. STelnet, based on the SSH protocol, provides powerful authentication functions to ensure information security and protect devices against attacks, such as IP spoofing attacks.	By default, you cannot log in to a device directly using STelnet. Before using STelnet to log in, you must locally log in to the device through a console port or mini USB port or remotely log in using Telnet and perform the following configurations: • Configure a reachable route between the user terminal and device. (By default, no management IP address is configured on the device.) • Enable the SSH server function and set parameters. • Configure a user interface for SSH login. • Configure an SSH user.

 Copyright © Huawei Technologies Co., Ltd.

Login Method	Advantages	Disadvantages	Applicable Scenario	Description
Logging In Through Redirection	Only remote serial port devices can be managed.	This login method applies only when two devices are connected through serial ports.	To manage a remote device that can transmit data only through a serial port, configure the redirection function on the router. The remote device can be a router, switch, or intelligent electricity meter that supports serial ports.	By default, the redirection function is disabled on a router. To use this function, configure the asynchronous serial port of the router to work in flow mode and enable the redirection function.
Logging In Through Reverse Telnet	Dumb terminals can only be directly connected to a router using asynchronous cables. The reverse Telnet function enables the dumb terminals to establish connections with a remote server through the router.	This login method applies only when two devices are connected through serial ports.	To connect dumb terminals that only have serial ports to a remote server, enable the reverse Telnet service on the router connected to the dumb terminals.	By default, the reverse Telnet function is disabled on a router. To use this function, configure the asynchronous port of the router to work in flow mode and configure parameters for connection between the dumb terminals remote server.

9.2 Overview of User Interfaces

The system supports console, TTY, and VTY user interfaces.

When a user logs in to a device through CLI, the system assigns a user interface to manage and monitor the session between the device and user. Each user interface has a user interface view, where you can set parameters, such as the authentication mode and user level. Users logging in through the user interface

 Copyright © Huawei Technologies Co., Ltd.

are restricted by these parameters. Through the parameter configuration, uniform management of various user sessions can be implemented.

The device supports three types of user interfaces:

- Console user interface: manages and monitors users who log in through the console port. A device provides the EIA/TIA-232 DCE console port. The serial port of a user terminal can be directly connected to the console port of the device for local access. The console user interface is also used to manage and monitor users who log in through a mini USB port.
- True type terminal (TTY) user interface: manages and monitors users who log in using TTY. The TTY mode is an asynchronous port login method, which can be implemented using the redirection or reverse Telnet function.
- Virtual type terminal (VTY) user interface: manages and monitors users who log in using VTY. A VTY connection is set up when a user uses Telnet or STelnet to log in to a device.

Relationship Between a User and a User Interface

A user interface is not exclusive to a specific user. User interfaces are used to manage and monitor users that have logged in to the device using a specific method. Although a user interface can only be used by one user at a time, the user interface is not specific to the user.

When a user logs in, the system allocates the idle user interface with the smallest number to the user based on the user's login mode. The login process is restricted by the configuration in the user interface view. For example, when user A logs in through the console port, the login process depends on the configuration in the console user interface view; however, when it logs in through VTY 1, the login process depends on the configuration in the VTY 1 user interface view. If a user logs in to a device using different methods, the user will be allocated different user interfaces. If a user logs in to a device at different time, the user may be allocated different user interfaces.

User Interface Numbering

User interfaces are numbered in either of the following modes:

- Relative numbering

  The numbering format is user interface type + number.

  This mode uniquely specifies a user interface or a group of user interfaces of the same type. Relative numbering adheres to the following rules:

  – Console user interface numbering: CON 0.

  – TTY user interface numbering: The first TTY user interface is TTY 1, the second TTY user interface is TTY 2, and so on

  – VTY user interface numbering: The first VTY user interface is VTY 0, the second VTY user interface is VTY 1, and so on.

- Absolute numbering

  This mode uniquely specifies a user interface or a group of user interfaces. You can run the **display user-interface** command to view user interfaces and their absolute numbers supported by the device.

 Copyright © Huawei Technologies Co., Ltd.

Each MPU supports only one console user interface and 15 VTY user interfaces. You can run the **user-interface maximum-vty** command in the system view to set the maximum number of VTY user interfaces. The default value is 5. By default, numbers VTY 16 to VTY 20 are reserved by the system and are unaffected by the **user-interface maximum-vty** command.

Table 9-2 lists the default absolute numbers of the console, TTY and VTY user interfaces.

Table 9-2 Default absolute numbers of the console and VTY user interfaces

User Interface	Description	Absolute Number	Relative Number
Console user interface	Manages and controls users who log in through the console port or mini USB port.	0	0
TTY user interface	Manages and controls users that log in to the device using an asynchronous serial interface.	1 to 128	The first TTY user interface is TTY 1, the second TTY user interface is TTY 2, and so on. Absolute numbers 1 to 128 map relative numbers TTY 1 to TTY 128.
VTY user interface	Manages and controls users who log in using Telnet or STelnet.	129 to 143	The first VTY user interface is VTY 0, the second VTY user interface is VTY 1, and so on. By default, VTY 0 to VTY 4 are available. Absolute numbers 129 to 143 map relative numbers VTY 0 to VTY 14.

Authentication Modes for User Interfaces

After you configure an authentication mode for a user interface, the system authenticates users before they access the user interface.

Two authentication modes are available: Authentication, Authorization, and Accounting (AAA) authentication and password authentication.

- AAA authentication: Users must enter both user names and passwords for login. If either a user name or a password is incorrect, the login fails.

 Copyright © Huawei Technologies Co., Ltd.

- Password authentication: Users must enter passwords for login. Only after a user enters the correct password does the device allow the users to log in.

User Levels for User Interfaces

You can manage login users based on their levels. The levels of commands accessible to a user depend on the user level.

- If password authentication is configured, the levels of commands accessible to a user depend on the level of the user interface through which the user logs in.
- If AAA authentication is configured, the levels of commands accessible to a user depend on the level of the local user specified in AAA configuration.

9.3 Licensing Requirements and Limitations for CLI Login

This section provides licensing requirements and limitations for CLI login.

Involved Network Elements

None

Licensing Requirements

CLI login configuration is a basic feature of a router and is not under license control.

Feature Limitations

For security purposes, after a user successfully logs in to a device in AAA mode, if the login password is the default password or the password changed using the change default-password command, the system displays the message Warning: The default password is not secure, and it is strongly recommended to change it. to prompt the user to change the default password.

The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

9.4 Configuring Login Through a Console Port

You can connect a PC to the console port of a device and then log in to the device to perform basic configurations and management.

 Copyright © Huawei Technologies Co., Ltd.

9.4.1 (Optional) Configuring Attributes for the Console User Interface

This section describes how to configure attributes about data transmission and screen display for the console user interface.

Context

The data transmission and screen display attributes of the console user interface are as follows:

- Data transmission attributes: transmission rate, flow control mode, parity bit, stop bit, and data bit. These attributes determine the data transmission mode used in the console port login process.
- Screen display attributes: timeout period of a connection, number of rows and columns displayed on a terminal screen, and buffer size for historical commands. These attributes determine terminal screen display for console port login.

Procedure

Step 1 Run **system-view**

The system view is displayed.

Step 2 Run **user-interface console 0**

The console user interface view is displayed.

Step 3 Configure data transmission attributes.

NOTE

The data transmission attributes configured on the terminal software must be the same as those on the device.

1. Run **speed** *speed-value*

   The transmission rate is set.

   The default transmission rate is 9600 bit/s.

2. Run **flow-control** { **hardware** | **none** }

   The flow control mode is set.

   The default flow control mode is set to none, indicating that the flow control function is not performed.

   NOTE

   AR100&AR120&AR150&AR160&AR200 series and AR2220E does not support this command.

3. Run **databits** { **7** | **8** }

   The data bit is set.

   The default data bit is 8. Data bit configuration depends on the code type used for information interchange. If standard ASCII codes are used, set the data bit to 7. If extended ASCII codes are used, set the data bit to 8.

 Copyright © Huawei Technologies Co., Ltd.

4. Run **parity** { **even** [**soft**] | **none** | **odd** [**soft**] }

   The parity bit is set.

   The default parity bit is set to none, indicating that the parity check is not performed on the console port. Setting a parity bit improves data security. If packets on the console port fail to pass the parity check, the device discards the packets.

5. Run **stopbits** { **1** | **1.5** | **2** }

   The stop bit is set.

   The default stop bit is 1. The stop bit indicates the end of a packet. More stop bits indicate lower transmission efficiency.

Step 4 Configure screen display attributes.

1. Run **idle-timeout** *minutes* [*seconds*]

   A timeout period is set for a user connection.

   If a connection remains idle for the specified timeout period, the system automatically ends the connection after the timeout period expires.

   The default timeout period is 5 minutes.

   NOTE

   If you set the timeout period of a terminal connection to 0 or too long, the terminal remains logged in to a device, which is a potential security risk. It is recommended that you run the **lock** command to lock the connection.

2. Run **screen-length** *screen-length*

   The number of rows displayed on a terminal screen is set.

   The default number of rows displayed on a terminal screen is 24.

   NOTE

   The system automatically adjusts the number of terminal screen lines.

3. Run **screen-width** *screen-width*

   The number of columns displayed on a terminal screen is set.

   The default number of columns displayed on a terminal screen is 80. Each character is a column.

4. Run **history-command max-size** *size-value*

   A buffer size is set for historical commands.

   The default buffer size is 10, that is, a maximum of 10 historical commands can be buffered.

----End

 Copyright © Huawei Technologies Co., Ltd.

9.4.2 Configuring an Authentication Mode for the Console User Interface

You can configure an authentication mode for the console user interface to control user access through the console port, which enhances login security.

Context

The system provides two authentication modes for the console user interface: AAA authentication and password authentication.

- AAA authentication: Users must enter both user names and passwords for login. If either a user name or a password is incorrect, the login fails.
- Password authentication: Users must enter passwords for login. Only after a user enters the correct password does the device allow the users to log in.

Procedure

- Configure AAA authentication.
  a. Run **system-view**

     The system view is displayed.
  b. Run **user-interface console 0**

     The console user interface view is displayed.
  c. Run **authentication-mode aaa**

     The authentication mode is set to AAA authentication.
  d. (Optional) run **authentication-domain** *domain-name*

     An authentication domain is configured.

     By default, the authentication domain is **default**. If you want to change the currently used authentication domain for users on the console user interface, you can run this command.
  e. Run **quit**

     Exit the console user interface view.
  f. Run **aaa**

     The AAA view is displayed.
  g. Run **local-user** *user-name* **password irreversible-cipher** *password*

     A local user account is created and a password is configured.
  h. Run **local-user** *user-name* **service-type terminal**

     The access type of the local user is set to **Console**.
  i. Run **quit**

     Exit the AAA view.
- Configure password authentication.
  a. Run **system-view**

     The system view is displayed.

 Copyright © Huawei Technologies Co., Ltd.

b. Run **user-interface console 0**

The console user interface view is displayed.

c. Run **authentication-mode password**

The authentication mode is set to password authentication.

d. Run **set authentication password cipher**

An authentication password is set.

----End

9.4.3 Configuring a User Level for the Console User Interface

This section describes how to configure a user level for the console user interface.

Context

- You can configure different user levels to control access rights of different users and improve device security.
- There are 16 user levels numbered from 0 to 15, in ascending order of priority.
- User levels map command levels. A user can use only the commands of the corresponding level or lower. **Table 9-3** describes mappings between user levels and command levels.

Table 9-3 Mappings between user levels and command levels

User Level	Command Level	Name	Description
0	0	Visit level	Commands of this level include commands used for network diagnosis such as ping and tracert commands, and remote access commands such as Telnet.
1	0 and 1	Monitoring level	Commands of this level are used for system maintenance, including display commands. **NOTE** Some display commands are not available at this level. For example, the **display current-configuration** and **display saved-configuration** commands are level-3 management commands. For details about command levels, see the *Huawei AR Series Access Routers Command Reference*.
2	0, 1, and 2	Configuration level	Commands of this level are used to configure network services provided directly to users, such as routing and commands of all network layers.

 Copyright © Huawei Technologies Co., Ltd.

User Level	Command Level	Name	Description
3 to 15	0, 1, 2, and 3	Management level	Commands of this level are used to control basic system operations and provide support for services, including file system, FTP, TFTP download, user management, command level setting, and debugging commands for fault diagnosis.

Procedure

Step 1 Run **system-view**

The system view is displayed.

Step 2 Run **user-interface console 0**

The console user interface view is displayed.

Step 3 Run **user privilege level** *level*

A user level is set.

By default, the users on the console user interface are at level 15.

- If the user level configured for a user interface conflicts with that configured for a user, the user level configured for the user takes precedence.
- If password authentication is configured, the levels of commands accessible to a user depend on the level of the console user interface through which the user logs in.
- If AAA authentication is configured, the levels of commands accessible to a user depend on the level of the local user specified in AAA configuration. By default, the level of a local user is 0 in AAA configuration. You can run the **local-user** *user-name* **privilege level** *level* command in the AAA view to change the level of the local user in AAA configuration.

----End

9.4.4 Logging In to a Device Through the Console Port

You can connect a PC to the console port of a device and then log in to the device.

Context

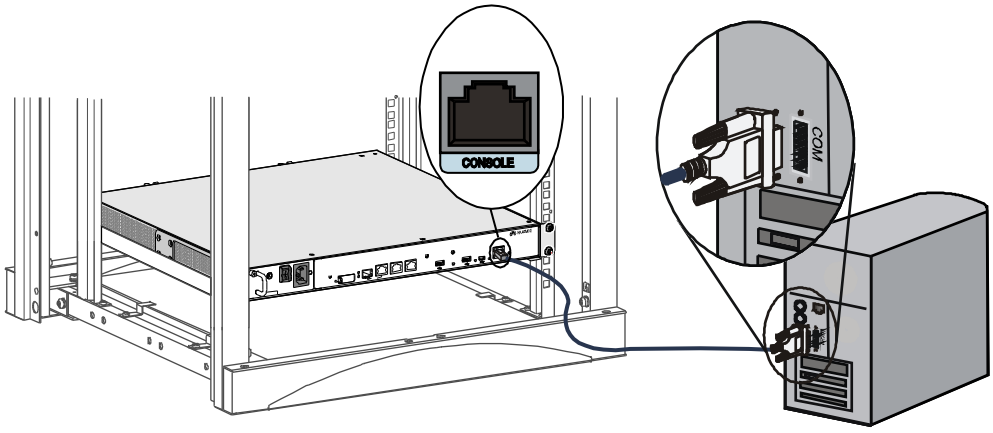
After completing console user interface configurations on a device, you can log in to the device through the console port. If the console user interface uses the default attribute settings and password authentication, perform the following steps to log in to the device.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Connect the DB9 female connector of the console cable to the COM port on the PC, and connect the RJ45 connector to the console port on the device, as shown in **Figure 9-1**.

Figure 9-1 Connecting to the device through the console port

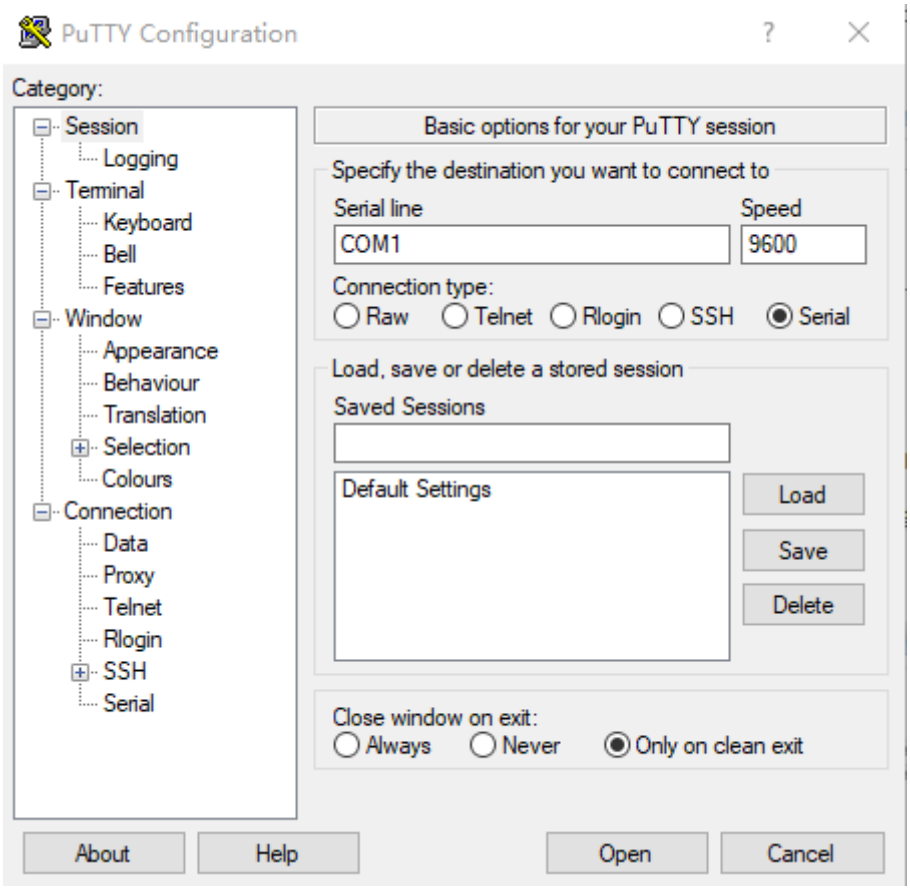


Step 2 Start the terminal emulation software on the PC. Create a connection, select the connected port, and set communication parameters. (This section uses the third-party software PuTTY as an example.)

1. Click  to establish a connection, as shown in **Figure 9-2**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 9-2 Establishing a connection



2. Set the connected port and communication parameters, as shown in **Figure 9-3**.

   Select the connected port based on actual situations. For example, you can view port information in **Device Manager** in the Windows operating system, and select the connected port.

   Communication parameters of the terminal emulation software must be consistent with the default attribute settings of the console user interface on the device, which are 9600 bit/s baud rate, 8 data bits, 1 stop bit, no parity check, and no flow control.

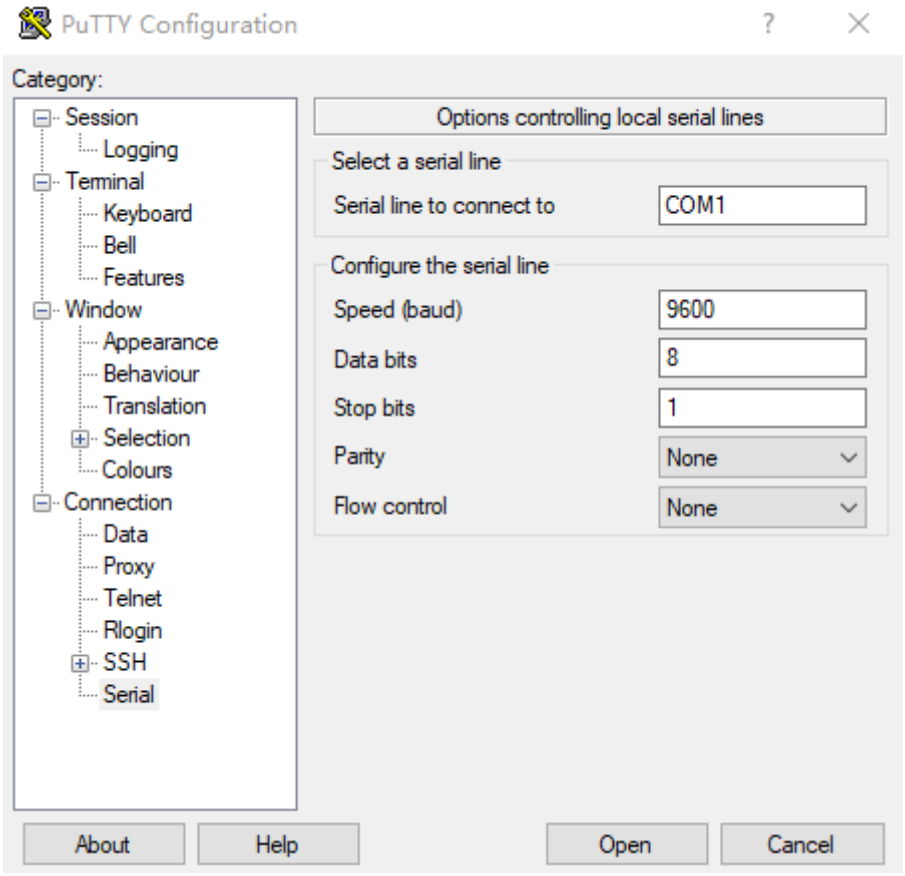
   NOTE

   By default, no flow control mode is configured on the device. Because RTS/CTS is selected in the software by default, you need to deselect RTS/CTS; otherwise, you cannot enter commands.

   If you modify the serial port communication parameters on the device, you must make the same modifications on the PC and then create a connection again.

 Copyright © Huawei Technologies Co., Ltd.

Figure 9-3 Setting the connected port and communication parameters



Step 3 Click **Connect**. The following information is displayed, prompting you to enter a password. (In AAA authentication, the system prompts you to enter the user name and password. The following information is only for reference.)

```
Login authentication


Password:
<Huawei>
```

You can run commands to configure the device. Enter a question mark (?) whenever you need help.

----End

Verifying the Configuration

- Run the **display users** [**all**] command to check user login information on the user interface.
- Run the **display user-interface console 0** command to check user interface information.
- Run the **display local-user** command to check the local user attributes.
- Run the **display access-user** command to check information about online users.

 Copyright © Huawei Technologies Co., Ltd.

9.5 Configuring Login Through the Mini USB Port

You can connect a PC to the mini USB port of a device and then log in to the device to perform basic configurations and management.

9.5.1 (Optional) Configuring Attributes for the Console User Interface

This section describes how to configure attributes about data transmission and screen display for the console user interface.

Context

The data transmission and screen display attributes of the console user interface are as follows:

- Data transmission attributes: transmission rate, flow control mode, parity bit, stop bit, and data bit. These attributes determine the data transmission mode used in the MiniUSB port login process.
- Screen display attributes: timeout period of a connection, number of rows and columns displayed on a terminal screen, and buffer size for historical commands. These attributes determine terminal screen display for MiniUSB port login.

Procedure

Step 1 Run **system-view**

The system view is displayed.

Step 2 Run **user-interface console 0**

The console user interface view is displayed.

Step 3 Configure data transmission attributes.

NOTE

The data transmission attributes configured on the terminal software must be the same as those on the device.

1. Run **speed** *speed-value*

   The transmission rate is set.

   The default transmission rate is 9600 bit/s.

2. Run **flow-control** { **hardware** | **none** }

   The flow control mode is set.

   The default flow control mode is set to none, indicating that the flow control function is not performed.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

AR100&AR120&AR150&AR160&AR200 series and AR2220E does not support this command.

3. Run **databits** { **7** | **8** }

   The data bit is set.

   The default data bit is 8. Data bit configuration depends on the code type used for information interchange. If standard ASCII codes are used, set the data bit to 7. If extended ASCII codes are used, set the data bit to 8.

4. Run **parity** { **even** [**soft**] | **none** | **odd** [**soft**] }

   The parity bit is set.

   The default parity bit is set to none, indicating that the parity check is not performed on the console port. Setting a parity bit improves data security. If packets on the console port fail to pass the parity check, the device discards the packets.

5. Run **stopbits** { **1** | **1.5** | **2** }

   The stop bit is set.

   The default stop bit is 1. The stop bit indicates the end of a packet. More stop bits indicate lower transmission efficiency.

Step 4 Configure screen display attributes.

1. Run **idle-timeout** *minutes* [*seconds*]

   A timeout period is set for a user connection.

   If a connection remains idle for the specified timeout period, the system automatically ends the connection after the timeout period expires.

   The default timeout period is 5 minutes.

   NOTE

   If you set the timeout period of a terminal connection to 0 or too long, the terminal remains logged in to a device, which is a potential security risk. It is recommended that you run the **lock** command to lock the connection.

2. Run **screen-length** *screen-length*

   The number of rows displayed on a terminal screen is set.

   The default number of rows displayed on a terminal screen is 24.

   NOTE

   The system automatically adjusts the number of terminal screen lines.

3. Run **screen-width** *screen-width*

   The number of columns displayed on a terminal screen is set.

   The default number of columns displayed on a terminal screen is 80. Each character is a column.

4. Run **history-command max-size** *size-value*

 Copyright © Huawei Technologies Co., Ltd.

A buffer size is set for historical commands.

The default buffer size is 10, that is, a maximum of 10 historical commands can be buffered.

----End

9.5.2 Configuring an Authentication Mode for the Console User Interface

You can configure an authentication mode for the console user interface to control user access through the mini USB port, which enhances login security.

Context

The system provides two authentication modes for the console user interface: AAA authentication and password authentication.

- AAA authentication: Users must enter both user names and passwords for login. If either a user name or a password is incorrect, the login fails.
- Password authentication: Users must enter passwords for login. Only after a user enters the correct password does the device allow the users to log in.

Procedure

- Configure AAA authentication.
  a. Run **system-view**

     The system view is displayed.
  b. Run **user-interface console 0**

     The console user interface view is displayed.
  c. Run **authentication-mode aaa**

     The authentication mode is set to AAA authentication.
  d. (Optional) run **authentication-domain** *domain-name*

     An authentication domain is configured.

     By default, the authentication domain is **default**. If you want to change the currently used authentication domain for users on the console user interface, you can run this command.
  e. Run **quit**

     Exit the console user interface view.
  f. Run **aaa**

     The AAA view is displayed.
  g. Run **local-user** *user-name* **password irreversible-cipher** *password*

     A local user account is created and a password is configured.
  h. Run **local-user** *user-name* **service-type terminal**

     The access type of the local user is set to **Console**.

 Copyright © Huawei Technologies Co., Ltd.

i. Run **quit**

Exit the AAA view.

- Configure password authentication.
  a. Run **system-view**

  The system view is displayed.
  b. Run **user-interface console 0**

  The console user interface view is displayed.
  c. Run **authentication-mode password**

  The authentication mode is set to password authentication.
  d. Run **set authentication password cipher**

  An authentication password is set.

----End

9.5.3 Configuring a User Level for the Console User Interface

This section describes how to configure a user level for the console user interface.

Context

- You can configure different user levels to control access rights of different users and improve device security.
- There are 16 user levels numbered from 0 to 15, in ascending order of priority.
- User levels map command levels. A user can use only the commands of the corresponding level or lower. **Table 9-4** describes mappings between user levels and command levels.

Table 9-4 Mappings between user levels and command levels

User Level	Command Level	Name	Description
0	0	Visit level	Commands of this level include commands used for network diagnosis such as ping and tracert commands, and remote access commands such as Telnet.
1	0 and 1	Monitoring level	Commands of this level are used for system maintenance, including display commands. **NOTE** Some display commands are not available at this level. For example, the **display current-configuration** and **display saved-configuration** commands are level-3 management commands. For details about command levels, see the *Huawei AR Series Access Routers Command Reference*.

 Copyright © Huawei Technologies Co., Ltd.

User Level	Command Level	Name	Description
2	0, 1, and 2	Configuration level	Commands of this level are used to configure network services provided directly to users, such as routing and commands of all network layers.
3 to 15	0, 1, 2, and 3	Management level	Commands of this level are used to control basic system operations and provide support for services, including file system, FTP, TFTP download, user management, command level setting, and debugging commands for fault diagnosis.

Procedure

Step 1 Run **system-view**

The system view is displayed.

Step 2 Run **user-interface console 0**

The console user interface view is displayed.

Step 3 Run **user privilege level** *level*

A user level is set.

By default, the users on the console user interface are at level 15.

- If the user level configured for a user interface conflicts with that configured for a user, the user level configured for the user takes precedence.
- If password authentication is configured, the levels of commands accessible to a user depend on the level of the console user interface through which the user logs in.
- If AAA authentication is configured, the levels of commands accessible to a user depend on the level of the local user specified in AAA configuration. By default, the level of a local user is 0 in AAA configuration. You can run the **local-user** *user-name* **privilege level** *level* command in the AAA view to change the level of the local user in AAA configuration.

----End

9.5.4 Logging In to a Device Through the Mini USB Port

You can connect a PC to the mini USB port of a device and then log in to the device.

 Copyright © Huawei Technologies Co., Ltd.

Context

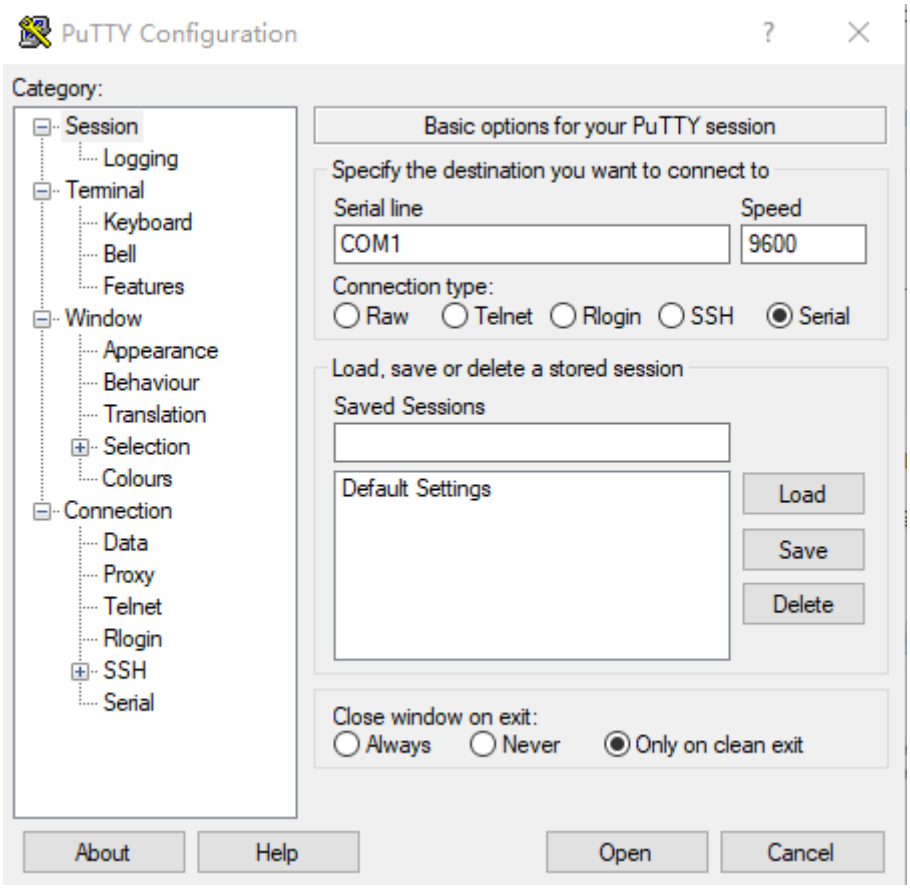
After completing console user interface configurations on a device, you can log in to the device through the mini USB port. If the console user interface uses the default attribute settings and password authentication.

Procedure

Step 1 Start the terminal emulation software on the PC. Create a connection, select the connected port, and set communication parameters. (This section uses the third-party software PuTTY as an example.)

1. Click  to establish a connection, as shown in **Figure 9-4**.

   Figure 9-4 Establishing a connection



2. Set the connected port and communication parameters, as shown in **Figure 9-5**.

   Select the connected port based on actual situations. For example, you can view port information in **Device Manager** in the Windows operating system, and select the connected port.

   Communication parameters of the terminal emulation software must be consistent with the default attribute settings of the console user interface on the device, which are 9600 bit/s baud rate, 8 data bits, 1 stop bit, no parity check, and no flow control.

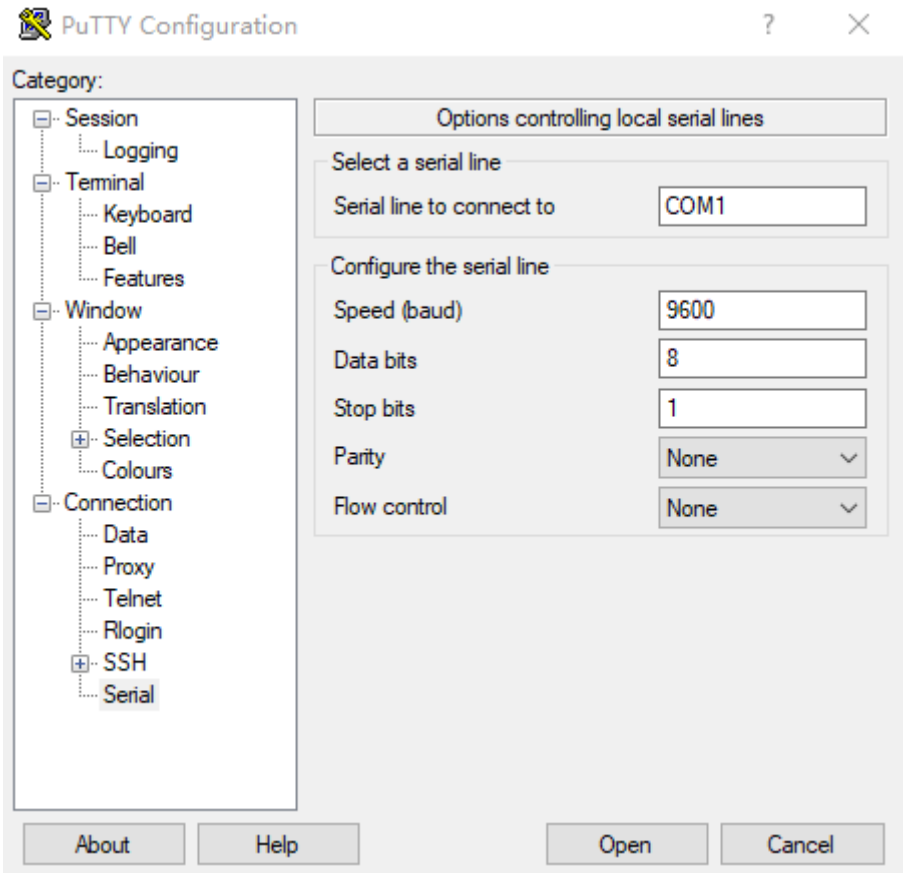
 Copyright © Huawei Technologies Co., Ltd.

NOTE

By default, no flow control mode is configured on the device. Because RTS/CTS is selected in the software by default, you need to deselect RTS/CTS; otherwise, you cannot enter commands.

If you modify the serial port communication parameters on the device, you must make the same modifications on the PC and then create a connection again.

Figure 9-5 Setting the connected port and communication parameters



Step 2 Click **Connect**. The following information is displayed, prompting you to enter a password. (In AAA authentication, the system prompts you to enter the user name and password. The following information is only for reference.)

```
Login authentication


Password:
<Huawei>
```

You can run commands to configure the device. Enter a question mark (?) whenever you need help.

----End

Verifying the Configuration

- Run the **display users** [**all**] command to check user login information on the user interface.

 Copyright © Huawei Technologies Co., Ltd.

- Run the **display user-interface console 0** command to check user interface information.
- Run the **display local-user** command to check the local user attributes.
- Run the **display access-user** command to check information about online users.

9.6 Configuring Telnet Login

You can log in to a device using Telnet to manage and configure the device.

NOTICE

The Telnet protocol has security vulnerabilities. It is recommended that you log in to the device using STelnet V2.

9.6.1 (Optional) Configuring Attributes for a VTY User Interface

This section describes how to configure attributes for a VTY user interface.

Context

You can configure attributes for a VTY user interface to control Telnet login and screen display. The attributes of a VTY user interface include the maximum number of VTY user interfaces, timeout period of a user connection, number of rows and columns displayed on a terminal screen, and buffer size for historical commands.

Procedure

Step 1 Run **system-view**

The system view is displayed.

Step 2 Run **user-interface maximum-vty** *number*

The maximum number of VTY user interfaces is set. The value determines the number of users that can concurrently log in to the device using Telnet or STelnet.

By default, the maximum number of VTY user interfaces is 5.

NOTE

- When the maximum number of VTY user interfaces is set to 0, no user (including Telnet and SSH users) can log in to the device through the VTY user interface, and web users cannot log in to the device through the web system either.
- If the configured maximum number is less than the current maximum number of online users, the system displays a configuration failure message.
- If the configured maximum number is greater than the current maximum number of online users, you need to configure an authentication mode for additional user interfaces.

 Copyright © Huawei Technologies Co., Ltd.

Step 3 Run **user-interface vty** *first-ui-number* [*last-ui-number*]

The VTY user interface view is displayed.

Step 4 Run **shell**

The VTY terminal service is enabled.

By default, all VTY terminal services are enabled. If you disable the terminal service of a VTY user interface, users cannot log in through the VTY user interface.

Step 5 Run **idle-timeout** *minutes* [*seconds*]

A timeout period is set for a user connection.

If a connection remains idle for the specified timeout period, the system automatically terminates the connection after the timeout period expires, which conserves system resources.

By default, the timeout period is 5 minutes.

NOTE

If you set the timeout period of a terminal connection to 0 or too long, the terminal remains logged in to a device, which is a potential security risk. It is recommended that you run the **lock** command to lock the connection.

Step 6 Run **screen-length** *screen-length* [**temporary**]

The number of rows displayed on a terminal screen is set.

If you specify **temporary** in the command, the configured value takes effect only on the current VTY user interface but does not take effect on the next login on the same user interface or login on other VTY user interfaces.

The default number of rows is 24.

Step 7 Run **screen-width** *screen-width*

The number of columns displayed on a terminal screen is set.

The default number of columns is 80. Each character is a column.

Step 8 Run **history-command max-size** *size-value*

A buffer size is set for historical commands.

The default buffer size is 10, that is, a maximum of 10 historical commands can be buffered.

----End

9.6.2 Configuring an Authentication Mode for a VTY User Interface

You can configure an authentication mode for a VTY user interface to control user access through Telnet, which enhances login security.

 Copyright © Huawei Technologies Co., Ltd.

Context

The system provides two authentication modes for a VTY user interface: AAA authentication and password authentication.

- AAA authentication: Users must enter both user names and passwords for login. If either a user name or a password is incorrect, the login fails.
- Password authentication: Users must enter passwords for login. Only after a user enters the correct password does the device allow the users to log in.

Procedure

- Configure AAA authentication.
  a. Run **system-view**

     The system view is displayed.
  b. Run **user-interface vty** *first-ui-number* [*last-ui-number*]

     The VTY user interface view is displayed.
  c. Run **protocol inbound** { **all** | **telnet** }

     The VTY user interface is configured to support the Telnet protocol.

     By default, a VTY user interface supports the SSH and Telnet protocol.
  d. Run **authentication-mode aaa**

     The authentication mode is set to AAA authentication.
  e. (Optional) run **authentication-domain** *domain-name*

     An authentication domain is configured.

     By default, the authentication domain is **default**. If you want to change the currently used authentication domain for users on the VTY user interface, you can run this command.
  f. Run **quit**

     Exit the VTY user interface view.
  g. Run **aaa**

     The AAA view is displayed.
  h. Run **local-user** *user-name* **password** { **cipher** | **irreversible-cipher** } *password*

     A local user account is created and a password is configured.
  i. Run **local-user** *user-name* **service-type telnet**

     The access type of the local user is set to **Telnet**.
  j. Run **quit**

     Exit the AAA view.
- Configure password authentication.
  a. Run **system-view**

     The system view is displayed.

 Copyright © Huawei Technologies Co., Ltd.

b. Run **user-interface vty** *first-ui-number* [*last-ui-number*]

The VTY user interface view is displayed.

c. Run **protocol inbound** { **all** | **telnet** }

The VTY user interface is configured to support the Telnet protocol.

By default, a VTY user interface supports the SSH and Telnet protocol.

d. Run **authentication-mode password**

The authentication mode is set to password authentication.

e. Run **set authentication password cipher**

An authentication password is set.

----End

9.6.3 Configuring a User Level for a VTY User Interface

This section describes how to configure a user level for a VTY user interface.

Context

- You can configure different user levels to control access rights of different users and improve device security.
- There are 16 user levels numbered from 0 to 15, in ascending order of priority.
- User levels map command levels. A user can use only the commands of the corresponding level or lower. **Table 9-5** describes mappings between user levels and command levels.

Table 9-5 Mappings between user levels and command levels

User Level	Command Level	Name	Description
0	0	Visit level	Commands of this level include commands used for network diagnosis such as ping and tracert commands, and remote access commands such as Telnet.
1	0 and 1	Monitoring level	Commands of this level are used for system maintenance, including display commands. **NOTE** Some display commands are not available at this level. For example, the **display current-configuration** and **display saved-configuration** commands are level-3 management commands. For details about command levels, see the *Huawei AR Series Access Routers Command Reference*.

 Copyright © Huawei Technologies Co., Ltd.

User Level	Command Level	Name	Description
2	0, 1, and 2	Configuration level	Commands of this level are used to configure network services provided directly to users, such as routing and commands of all network layers.
3 to 15	0, 1, 2, and 3	Management level	Commands of this level are used to control basic system operations and provide support for services, including file system, FTP, TFTP download, user management, command level setting, and debugging commands for fault diagnosis.

Procedure

Step 1 Run **system-view**

The system view is displayed.

Step 2 Run **user-interface vty** *first-ui-number* [*last-ui-number*]

The VTY user interface view is displayed.

Step 3 Run **user privilege level** *level*

A user level is set.

By default, the users on the VTY user interface are at level 0.

- If the user level configured for a user interface conflicts with that configured for a user, the user level configured for the user takes precedence.
- If password authentication is configured, the levels of commands accessible to a user depend on the level of the VTY user interface through which the user logs in.
- If AAA authentication is configured, the levels of commands accessible to a user depend on the level of the local user specified in AAA configuration. By default, the level of a local user is 0 in AAA configuration. You can run the **local-user** *user-name* **privilege level** *level* command in the AAA view to change the level of the local user in AAA configuration.

----End

9.6.4 Enabling the Telnet Server Function

In addition to the authentication mode and user level, you need to configure the Telnet server function on a device.

Context

When a device functions as a Telnet server, you can specify the protocol port and source interface of the Telnet server to enhance Telnet connection security.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Run **system-view**

The system view is displayed.

Step 2 Run **telnet** [**ipv6**] **server enable**

The Telnet server function is enabled.

By default, the Telnet server function is disabled on a device.

Step 3 (Optional) Run **telnet server port** *port-number*

The protocol port number is specified for the Telnet server.

By default, the protocol port number of the Telnet server is 23.

You can configure a new protocol port number for a Telnet server to prevent attackers from accessing the server using the default port.

Step 4 (Optional) Run **telnet server permit interface** { *interface-type interface-number* } &<1-5>

The physical interfaces on the Telnet server to which clients can connect is specified.

Step 5 (Optional) Run **telnet server-source** { **-a** [**ipv6**] *source-ip-address* | **-i** [**ipv6**] *interface-type interface-number* }

The source interface is specified for the Telnet server.

By default, the source interface of a Telnet server is not specified.

If the source IP address is not specified for the Telnet server, the device selects a source IP address according to routing entries to send packets. Specify an interface in stable state, such as a loopback interface, as the source interface. Before specifying a source interface, make sure that the Telnet client has a reachable route to the source interface. Otherwise, the configuration will fail.

Step 6 (Optional) Configure ACL-based Telnet access control.

- Control access to the local device.
  a. Run **acl** *acl-number*

     An ACL is created, and the ACL view is displayed.

     acl-number refers to a basic ACL numbered from 2000 to 2999.
  b. Run **rule permit source** *source-address* **0**

     ACL rules are configured to prohibit devices except the device specified by *source-address* from accessing the local device.
  c. Run **quit**

     Exit the ACL view.
  d. Run **user-interface vty** *first-ui-number* [*last-ui-number*]

     The VTY user interface view is displayed.
  e. Run **acl** [**ipv6**] *acl-number* **inbound**

     The ACL-based Telnet access control is configured for the VTY user interface.

 Copyright © Huawei Technologies Co., Ltd.

- Control access of the local device to other devices.
  a. Run **acl** *acl-number*

     An ACL is created, and the ACL view is displayed.

     acl-number refers to an advanced ACL numbered from 3000 to 3999.
  b. Run **rule deny tcp destination-port eq telnet**

     ACL rules are configured to prohibit the local device from accessing other devices.
  c. Run **quit**

     Exit the ACL view.
  d. Run **user-interface vty** *first-ui-number* [*last-ui-number*]

     The VTY user interface view is displayed.
  e. Run **acl** [**ipv6**] *acl-number* **outbound**

     The ACL-based Telnet access control is configured for the VTY user interface.

----End

9.6.5 Logging In to a Device Through Telnet

This section describes how to log in to a device using Telnet.

Context

After completing Telnet server configurations on a device, you can use either Telnet software or Windows Command Prompt on a PC to log in to the device. Assume that AAA authentication is configured and the management IP address of the device is 10.137.217.177. The Windows Command Prompt is used as an example to illustrate the Telnet login process.

Procedure

Step 1 Enter the Windows Command Prompt window.

Step 2 Run the **telnet** *ip-address* command to log in to the device using Telnet.

```
C:\Documents and Settings\Administrator> telnet 10.137.217.177
```

Step 3 Press **Enter** and enter the password and user name configured for AAA authentication. The system does not provide a default user name and password. If authentication succeeds, the CLI is displayed, indicating that you have successfully logged in to the device. (The following information is for reference only.)

```
Login authentication

Username:admin1234
Password:
<Telnet Server>
```

----End

Verifying the Configuration

- Run the **display users** [**all**] command to check the user interface connections.

 Copyright © Huawei Technologies Co., Ltd.

- Run the **display tcp status** command to check all TCP connections.
- Run the **display telnet server status** command to check current Telnet server connections.

9.6.6 (Optional) Using Telnet to Log In to Another Device From the Local Device

This section describes how to use Telnet to log in to another device from the local device.

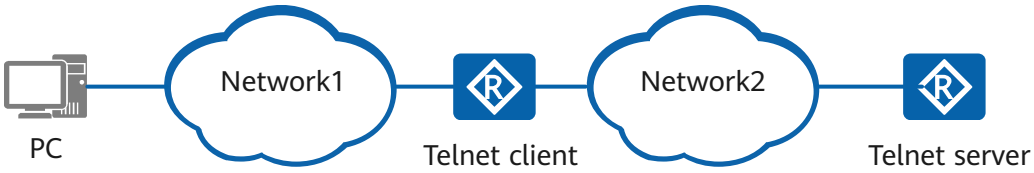
Context

A device can function as a Telnet server to allow other devices to log in or as a Telnet client to log in to other devices. When a terminal lacks the necessary software or no reachable route exists between the terminal and target device, you can log in to an intermediate device and then use Telnet to log in to the target device from the intermediate device. The intermediate device functions as a Telnet client.

The device can function as a Telnet IPv6 client. You can specify the source address or interface of the Telnet client to ensure security of the management IP address.

As shown in **Figure 9-6**, a PC connects to a device through network 1 and the device connects to a Telnet server through network 2. The PC cannot directly communicate with the Telnet server. In this situation, you can configure the device as a Telnet client and log in to the Telnet server from the device.

Figure 9-6 Configuring a device as a Telnet client to log in to another device



Pre-configuration Tasks

Before configuring a device as a Telnet client to log in to another device, complete the following tasks:

- Log in to the device from a terminal.
- Configure a reachable route between the device and Telnet server.
- Enable the Telnet server function on the Telnet server.
- Obtain the Telnet user name, password, and port number configured on the Telnet server.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Run **system-view**

The system view is displayed.

Step 2 (Optional) Run **telnet client-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* }

The source IP address of the Telnet client is set.

The source address of the Telnet client displayed on the server is the same as that configured in this step.

Step 3 Run **quit**

Exit the system view.

Step 4 Run either of the following commands to log in to another device based on the network address type.

- In IPv4 mode, run the **telnet** [**-a** *source-ip-address*] *host-ip* [*port-number*] command to log in to another device as a Telnet client.
- In IPv6 mode, run the **telnet ipv6** [**-a** *source-ip-address*] *host-ipv6* [**-oi** *interface-type interface-number*] [*port-number*] command to log in to another device as a Telnet IPv6 client.

----End

9.7 Configuring STelnet Login

You can log in to a device using STelnet to manage and configure the device.

NOTE

The STelnet V1 protocol has security vulnerabilities. It is recommended that you log in to the device using STelnet V2.

9.7.1 (Optional) Configuring Attributes for a VTY User Interface

This section describes how to configure attributes for a VTY user interface.

Context

You can configure attributes for a VTY user interface to control STelnet login and screen display. The attributes of a VTY user interface include the maximum number of VTY user interfaces, timeout period of a user connection, number of rows and columns displayed on a terminal screen, and buffer size for historical commands.

Procedure

Step 1 Run **system-view**

The system view is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Step 2 Run **user-interface maximum-vty** *number*

The maximum number of VTY user interfaces is set. The value determines the number of users that can concurrently log in to the device using Telnet or STelnet.

By default, the maximum number of VTY user interfaces is 5.

NOTE

- When the maximum number of VTY user interfaces is set to 0, no user (including Telnet and SSH users) can log in to the device through the VTY user interface, and web users cannot log in to the device through the web system either.
- If the configured maximum number is less than the current maximum number of online users, the system displays a configuration failure message.
- If the configured maximum number is greater than the current maximum number of online users, you need to configure an authentication mode for additional user interfaces.

Step 3 Run **user-interface vty** *first-ui-number* [*last-ui-number*]

The VTY user interface view is displayed.

Step 4 Run **shell**

The VTY terminal service is enabled.

By default, all VTY terminal services are enabled. If you disable the terminal service of a VTY user interface, users cannot log in through the VTY user interface.

Step 5 Run **idle-timeout** *minutes* [*seconds*]

A timeout period is set for a user connection.

If a connection remains idle for the specified timeout period, the system automatically terminates the connection after the timeout period expires, which conserves system resources.

By default, the timeout period is 5 minutes.

NOTE

If you set the timeout period of a terminal connection to 0 or too long, the terminal remains logged in to a device, which is a potential security risk. It is recommended that you run the **lock** command to lock the connection.

Step 6 Run **screen-length** *screen-length* [**temporary**]

The number of rows displayed on a terminal screen is set.

If you specify **temporary** in the command, the configured value takes effect only on the current VTY user interface but does not take effect on the next login on the same user interface or login on other VTY user interfaces.

The default number of rows is 24.

Step 7 Run **screen-width** *screen-width*

The number of columns displayed on a terminal screen is set.

The default number of columns is 80. Each character is a column.

Step 8 Run **history-command max-size** *size-value*

 Copyright © Huawei Technologies Co., Ltd.

A buffer size is set for historical commands.

The default buffer size is 10, that is, a maximum of 10 historical commands can be buffered.

----End

9.7.2 Configuring an Authentication Mode for a VTY User Interface

You can configure an authentication mode for a VTY user interface to control user access through STelnet, which enhances login security.

Context

To configure a VTY user interface to support SSH, you must set the authentication mode of the VTY user interface to AAA; otherwise, the **protocol inbound ssh** command does not take effect.

Procedure

Step 1 Run **system-view**

The system view is displayed.

Step 2 Run **user-interface vty** *first-ui-number* [*last-ui-number*]

The VTY user interface view is displayed.

Step 3 Run **authentication-mode aaa**

The authentication mode is set to AAA authentication.

Step 4 (Optional) run **authentication-domain** *domain-name*

An authentication domain is configured.

By default, the authentication domain is **default**. If you want to change the currently used authentication domain for users on the VTY user interface, you can run this command.

Step 5 (Optional) If you want to change the currently used authentication domain for users on the VTY user interface, run **authentication-domain** *domain-name*

An authentication domain is configured.

By default, the authentication domain is **default**.

Step 6 Run **protocol inbound** { **all** | **ssh** }

The VTY user interface is configured to support the SSH protocol.

By default, a VTY user interface supports the SSH and Telnet protocol.

Step 7 Run **quit**

Return to the system view.

Step 8 Run **ssh user** *user-name* **authentication-type** { **password** | **rsa** | **password-rsa** | **ecc** | **password-ecc** |**all** }**rsa peer-public-key** or **ecc peer-public-key***key-name*

 Copyright © Huawei Technologies Co., Ltd.

public-key-code beginpublic-key-code endpeer-public-key endssh user *user-name* **assign** { **rsa-key** | **ecc-key** } *key-name*

An authentication mode is set for the SSH user.

----End

9.7.3 Configuring a User Level for a VTY User Interface

This section describes how to configure a user level for a VTY user interface.

Context

- You can configure different user levels to control access rights of different users and improve device security.
- There are 16 user levels numbered from 0 to 15, in ascending order of priority.
- User levels map command levels. A user can use only the commands of the corresponding level or lower. **Table 9-6** describes mappings between user levels and command levels.

Table 9-6 Mappings between user levels and command levels

User Level	Command Level	Name	Description
0	0	Visit level	Commands of this level include commands used for network diagnosis such as ping and tracert commands, and remote access commands such as Telnet.
1	0 and 1	Monitoring level	Commands of this level are used for system maintenance, including display commands. **NOTE** Some display commands are not available at this level. For example, the **display current-configuration** and **display saved-configuration** commands are level-3 management commands. For details about command levels, see the *Huawei AR Series Access Routers Command Reference*.
2	0, 1, and 2	Configuration level	Commands of this level are used to configure network services provided directly to users, such as routing and commands of all network layers.
3 to 15	0, 1, 2, and 3	Management level	Commands of this level are used to control basic system operations and provide support for services, including file system, FTP, TFTP download, user management, command level setting, and debugging commands for fault diagnosis.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

- If a user uses password authentication mode, the user level is configured in the AAA view.
  a. Run **system-view**
     The system view is displayed.
  b. Run **aaa**
     The AAA view is displayed.
  c. Run **local-user** *user-name* **privilege level** *level*
     The local user level is configured.
  d. Run **quit**
     Return to the system view.
- If a user uses RSA or ECC authentication mode, the user level is determined by the user level of the VTY interface to which the user logs in.
  a. Run **system-view**
     The system view is displayed.
  b. Run **user-interface vty** *first-ui-number* [*last-ui-number*]
     The VTY user interface view is displayed.
  c. Run **user privilege level** *level*
     The user level is configured for the VTY user interface.
     By default, the user level of a VTY user interface is 0.

  NOTE

  - If an SSH user uses all authentication mode and an AAA user with the same name as the SSH user exists, user levels may be different in password, RSA and ECC authentication modes. Configure the user level based on actual requirements.
  - If the user level configured for a user interface conflicts with that configured for a user, the user level configured for the user takes precedence.

----End

9.7.4 Configuring an SSH User

To use STelnet to log in to a device, you need to configure an SSH user. In addition to setting AAA authentication for the VTY user interface, you also need to specify an authentication mode for the SSH user.

Context

SSH users can be authenticated in the following modes: password, Revest-Shamir-Adleman Algorithm (RSA), Elliptic Curves Cryptography (ECC), password-RSA, Password-ECC and all.

- Password authentication: is based on the user name and password. You need to configure a password for each SSH user in the AAA view. A user must enter the correct user name and password to log in using SSH.
- Rivest-Shamir-Adleman Algorithm (RSA) authentication: is based on the private key of the client. RSA is a public-key cryptographic system that uses an asymmetric encryption algorithm. An RSA key pair consists of a public key

 Copyright © Huawei Technologies Co., Ltd.

and a private key. You need to copy the public key generated by the client to the SSH server. The SSH server then uses the public key to encrypt data. A maximum of 20 keys can be stored on a device functioning as an SSH client.

- Elliptic Curves Cryptography (ECC) authentication: is an elliptic curve algorithm. Compared with RSA, ECC features shorter key length, lower computational cost, faster processing speed, smaller storage space, and lower bandwidth requirement under the same security performance.
- Password-RSA authentication: The SSH server implements both password and RSA authentication on login users. The users must pass both authentication modes to log in.
- Password-ECC authentication: The SSH server implements both password and ECC authentication on login users. The users must pass both authentication modes to log in.
- All authentication: The SSH server implements RSA, ECC or password authentication on login users. Users only need to pass either of them to log in.

Procedure

Step 1 Run **system-view**

The system view is displayed.

Step 2 Configure AAA user information.

1. Run **aaa**

   The AAA view is displayed.
2. Run **local-user** *user-name* **password** { **cipher** | **irreversible-cipher** } *password*

   A local user is created and a password is configured.
3. Run **local-user** *user-name* **privilege level** *level*

   A user level is set for the local user.
4. Run **local-user** *user-name* **service-type ssh**

   A service type is set for the local user.
5. Run **quit**

   Return to the system view.

Step 3 (Optional) Run **ssh user default-authentication-type** { **password** | **rsa** }

The default authentication mode is configured for SSH users.

By default, the default authentication mode for SSH users is password authentication except AR161EW, AR161EW-M1, AR169EW, AR169EGW-L, AR2204XE-DC, and AR2204XE. By default, the default authentication mode for SSH users of the AR161EW, AR161EW-M1, AR169EW, AR169EGW-L, AR2204XE-DC, and AR2204XE is RSA authentication.

Step 4 Run **ssh user** *user-name* **authentication-type** { **password** | **rsa** | **password-rsa** | **ecc** | **password-ecc** |**all** }

An authentication mode is set for the SSH user.

- If password authentication is used, the SSH user is the user with the same name as the local user configured in the AAA view.

 Copyright © Huawei Technologies Co., Ltd.

- If RSA or ECC authentication is used, you need to configure the public key generated by the SSH client on the SSH server. When the SSH client logs in to the SSH server, the SSH client passes the authentication if the private key of the client matches the configured public key.

  NOTE

  In RSA or ECC authentication mode, the user level configured in the VTY user interface view takes effect.

  a. Run **rsa peer-public-key** *key-name* or **ecc peer-public-key** *key-name*

     The RSA or ECC public key view is displayed.

  b. Run **public-key-code begin**

     The public key editing view is displayed.

  c. Enter the public key of the SSH client.

     The entered public key must be a hexadecimal string complying with the public key format. The string is generated by SSH client software. For detailed operations, see the help document of the SSH client software.

  d. Run **public-key-code end**

     Exit the public key editing view.

  e. Run **peer-public-key end**

     Return to the system view from the public key view.

  f. Run **ssh user** *user-name* **assign** { **rsa-key** | **ecc-key** } *key-name*

     An RSA or ECC public key is allocated to the SSH user. When logging in to the server, the client enters the SSH user name corresponding to its public key as prompted.

- If Password-RSA or Password-ECC authentication is used, configure AAA user information and enter the public key generated on the client.
- If all authentication is used, configure AAA user information or enter the public key generated on the client or perform the two operations together.

----End

9.7.5 Enabling the SSH Server Function

To allow user terminals to establish an SSH connection with a device, log in to the device in another mode and enable the SSH server function on the device.

Context

A device serving as an SSH server must generate a key pair of the same type as the client's key for data encryption and server authentication on the client. The device also supports configuration of rich SSH server attributes for flexible control on SSH login.

Procedure

Step 1 Run **system-view**

The system view is displayed.

Step 2 Run **stelnet server enable**

The SSH server function is enabled on the device.

By default, the SSH server function is disabled.

Step 3 (Optional) Run **ssh server cipher** { **3des_cbc** | **aes128_cbc** | **aes128_ctr** | **aes192_ctr** | **aes256_ctr** | **blowfish_cbc** | **des_cbc** }*

An encryption algorithm list is configured for the SSH server.

Earlier versions of V200R010C10:

By default, algorithms except **des_cbc** are included in the encryption algorithm list of the SSH server.

V200R010C10 and later versions:

By default, an SSH server supports the following encryption algorithms: **aes128_ctr**, **aes192_ctr**, and **aes256_ctr**.

The server and client negotiate the algorithm for encrypting packets transmitted between them. You can run the **ssh server cipher** command to configure the encryption algorithm list of the SSH server. The server compares the encryption algorithm list sent from the client with its own encryption algorithm list, and selects the first matched encryption algorithm for encrypting transmitted packets. If the encryption algorithm lists of the server and client have no common encryption algorithm, the encryption algorithm negotiation fails.

NOTE

You are advised not to add the following encryption algorithms to the encryption algorithm list of the SSH server because they provide low security: **3des_cbc**, **aes128_cbc**, **blowfish_cbc**, and **des_cbc**.

Step 4 (Optional) Run **ssh server hmac** { **md5** | **md5_96** | **sha1** | **sha1_96** | **sha2_256** | **sha2_256_96** }*

A check algorithm list is configured for the SSH server.

Earlier versions of V200R010C10:

By default, an SSH server supports all the check algorithms.

V200R010C10 and later versions:

By default, an SSH server supports the **sha2_256** encryption algorithms only.

The server and client negotiate the algorithm for checking packets transmitted between them. You can run the **ssh server hmac** command to configure the check algorithm list of the SSH server. The server compares the check algorithm list sent from the client with its own check algorithm list, and selects the first matched check algorithm for checking transmitted packets. If the check algorithm lists of the server and client have no common check algorithm, the check algorithm negotiation fails.

NOTE

You are advised not to add the following HMAC check algorithms to the HMAC check algorithm list of the SSH server because they provide low security: **sha2_256_96**, **sha1**, **sha1_96**, **md5**, and **md5_96**.

 Copyright © Huawei Technologies Co., Ltd.

Step 5 (Optional) Run **ssh server key-exchange** { **dh_group_exchange_sha1** | **dh_group14_sha1** | **dh_group1_sha1** } *

A key exchange algorithm list is configured for the SSH server.

Earlier versions of V200R010C10:

By default, an SSH server supports all key exchange algorithms.

V200R010C10 and later versions:

By default, an SSH server supports the following key exchange algorithms: **dh_group_exchange_sha1** and **dh_group14_sha1**.

During the negotiation process, the client and server negotiate the key exchange algorithm for packet transmission. You can perform this step to configure a key exchange algorithm list for the SSH server. The server compares the key exchange algorithm list sent by the client with its own key exchange algorithm list, and selects the first key exchange algorithm on the client's list that matches a key exchange algorithm on its own list as the key exchange algorithm for packet transmission. If no algorithm on the client's list matches an algorithm on the server's list, the negotiation fails.

NOTE

You are advised not to add the **dh_group1_sha1** algorithm to the key exchange algorithm list of the SSH server because it provides low security.

Step 6 Run **rsa local-key-pair create** or**ecc local-key-pair create**

A local RSA or ECC key pair is generated.

NOTE

A longer key pair indicates higher security. It is recommended that you use the maximum key pair length.

Step 7 (Optional) Run **ssh server port** *port-number*

The port number of the SSH server is specified.

By default, the port number of the SSH server is 22.

Configuring a port number for an SSH server can prevent attackers from accessing the SSH server using the default port, improving SSH server security.

Step 8 (Optional) Run **ssh server rekey-interval** *hours*

The interval for updating key pairs is set.

The default interval is 0, indicating that the key pairs are never updated.

An SSH server automatically updates key pairs at the configured intervals, which ensures security.

Step 9 (Optional) Run **ssh server timeout** *seconds*

The timeout period is set for SSH authentication.

The default timeout period is 60 seconds.

 Copyright © Huawei Technologies Co., Ltd.

If a user fails to log in within the timeout period for SSH authentication, the device disconnects the current connection to ensure system security.

Step 10 (Optional) Run **ssh server authentication-retries** *times*

The maximum number of SSH authentication retries is set.

The default maximum number of SSH authentication retries is 3.

You can set the maximum number of SSH authentication retries to prevent unauthorized access.

Step 11 (Optional) Run **ssh server compatible-ssh1x enable**

Compatibility with earlier SSH versions is enabled.

By default, compatibility with earlier SSH versions is disabled on an unconfigured device. When a device is upgraded to a later version, the configuration of the compatibility function is the same as that specified in the configuration file.

NOTE

If the SSH server is enabled to be compatible with earlier SSH versions, the system prompts a security risk.

Step 12 (Optional) Run **telnet server-source** { **-a** [**ipv6**] *source-ip-address* | **-i** [**ipv6**] *interface-type interface-number* }

The source interface is specified for the SSH server.

By default, the source interface of a SSH server is not specified.

If the source IP address is not specified for the SSH server, the device selects a source IP address according to routing entries to send packets. Specify an interface in stable state, such as a loopback interface, as the source interface. Before specifying a source interface, make sure that the SSH client has a reachable route to the source interface. Otherwise, the configuration will fail.

Step 13 (Optional) Run **ssh server permit interface** { *interface-type interface-number* } &<1-5>

The physical interfaces on the SSH server to which clients can connect is specified.

By default, clients can connect to all the physical interfaces on the SSH server.

To prevent a client from connecting to the SSH server through an unauthorized physical interface, you can run the command to specify physical interfaces on the SSH server to which the client can connect.

----End

9.7.6 Logging In to a Device Through STelnet

This section describes how to log in to a device using STelnet.

Context

After completing SSH user and STelnet server configurations on a device, you can use STelnet software on a PC to log in to the device. Assume that password authentication is configured for SSH users and the management IP address of the

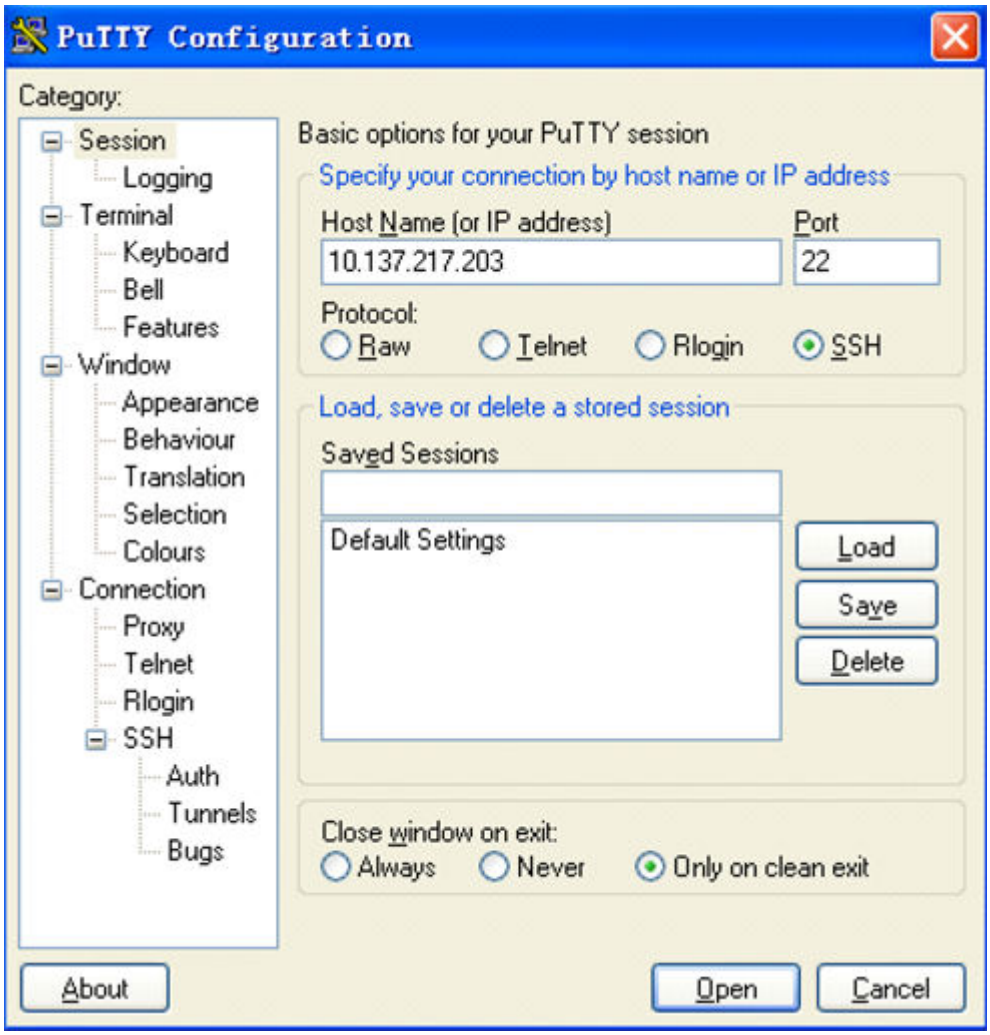
 Copyright © Huawei Technologies Co., Ltd.

device is 10.137.217.203. The third-party software, PuTTY, is used as an example to illustrate the STelnet login process.

Procedure

Step 1 Start the PuTTY software, enter the device's IP address and port and select the SSH protocol.

Figure 9-7 Logging in to an SSH server through PuTTY in password authentication mode



Step 2 Click **Open**. In the displayed page, enter the user name and password and press **Enter** to log in to the device through STelnet.

```
login as: client001      //Enter the SSH user name.
Sent username "client001"

client001@10.137.217.203's password:          //Enter the password configured through AAA.

<SSH Server>
```

----End

 Copyright © Huawei Technologies Co., Ltd.

Verifying the Configuration

- Run the **display ssh user-information** [*username*] command to check information about SSH users on the SSH server. If no SSH user is specified, information about all SSH users logging in to the SSH server is displayed.
- Run the **display ssh server status** command to check global configurations of the SSH server.
- Run the **display ssh server session** command to check information about sessions between the SSH server and client.

9.7.7 (Optional) Using STelnet to Log In to Another Device from the Local Device

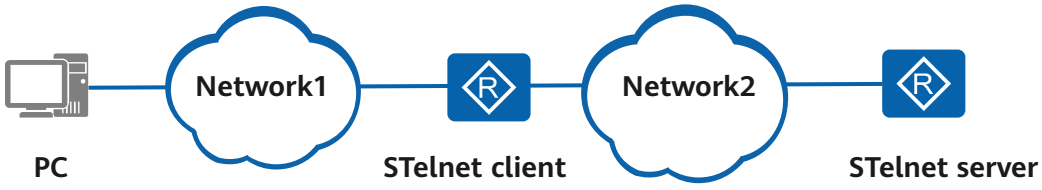
This section describes how to use STelnet to log in to another device from the local device.

Context

A device can function as both an STelnet server and an STelnet client. As an STelnet client, the device can log in to other devices. When a terminal lacks the necessary software or no reachable route exists between the terminal and target device, you can log in to an intermediate device and then use STelnet to log in to the target device from the intermediate device. The intermediate device functions as an STelnet client.

As shown in **Figure 9-8**, a PC connects to a device through network 1 and the device connects to an STelnet server through network 2. The PC cannot directly communicate with the STelnet server. In this situation, you can configure the device as an STelnet client and log in to the STelnet server from the device.

Figure 9-8 Configuring a device as an STelnet client to log in to another device



Pre-configuration Tasks

Before configuring a device as an STelnet client to log in to another device, complete the following tasks:

- Log in to the device from a terminal.
- Configure a reachable route between the device and STelnet server.
- Enable the STelnet server function on the STelnet server.
- Obtain the SSH user name and password, server keys, and port number configured on the STelnet server.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Generate a local key pair for the SSH client.

1. Run **system-view**

   The system view is displayed.

2. Run **rsa local-key-pair create**, or **ecc local-key-pair create**

   A local RSA or ECC key pair is generated. The generated key pair must be of the same type as that of the server.

   You can run the **display rsa local-key-pair public** or **display ecc local-key-pair public** command to view information about the public key in the generated RSA or ECC key pair. Configure the public key on the SSH server. For details, see **9.7.4 Configuring an SSH User**.

3. Run **quit**

   Return to the user view.

Step 2 Configure the mode in which the device connects to the SSH server for the first time.

When working as an SSH client to connect to an SSH server for the first time, the device cannot validate the SSH server because the public key of the SSH server has not been saved on the client. As a result, the connection fails. You can perform either of the following operations to rectify the connection failure:

- Enable first-time authentication on the SSH client. This function allows the device to successfully connect to an SSH server for the first time without validating the SSH server's public key. If saving the SSH server's public key is selected during server authentication, the device automatically saves the SSH server's public key after connecting to the server successfully for subsequent server authentication. If saving the SSH server's public key is not selected, the system asks you whether to save the SSH server's public key the next time server authentication is performed.

  a. Run **system-view**

     The system view is displayed.

  b. Run **ssh client first-time enable**

     First-time authentication is enabled on the SSH client.

     By default, first-time authentication is disabled on an SSH client.

- Configure the SSH client to assign a public key to the SSH server. In this mode, the public key generated on the server is directly saved on the client to ensure that the SSH server passes the validity check on the client's first login.

  a. Run **system-view**

     The system view is displayed.

  b. Run **rsa peer-public-key** *key-name* [**encoding-type** { **der** | **openssh** | **pem** }] or **ecc peer-public-key** *key-name* **encoding-type** { **der** | **openssh** | **pem** }

     The RSA or ECC public key view is displayed.

  c. Run **public-key-code begin**

     The public key editing view is displayed.

 Copyright © Huawei Technologies Co., Ltd.

d. Enter the public key of the SSH server.

The entered public key must be a hexadecimal string complying with the public key format. The string is randomly generated on the SSH server.

After entering the public key editing view, you can enter the RSA or ECC public key generated by the server on the client.

e. Run **public-key-code end**

Exit the public key editing view.

f. Run **peer-public-key end**

Exit the public key view.

g. Run **ssh client** *servername* **assign** { **rsa-key**| **ecc-key** } *key-name*

The RSA or ECC public key is bound to the SSH server.

NOTE

If the SSH server's public key saved on the SSH client does not take effect, run the **undo ssh client** *servername* **assign** { **rsa-key** | **ecc-key** } command to unbind the RSA or ECC public key from the SSH server and then run the command to assign a new RSA or ECC public key to the SSH server.

Step 3 Log in to another device.

Run either of the preceding commands based on the network address type.

- IPv4 mode:

  run the **stelnet** [**-a** *source-address*] *host-ip* [*port-number*] [[**-vpn-instance** *vpn-instance-name*] | [**prefer_kex** { **dh_group1** | **dh_exchange_group** }] | [**prefer_ctos_cipher** { **des** | **3des** | **aes128** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** }] | [**prefer_ctos_hmac** { **sha1** }] | [**prefer_stoc_cipher** { **des** | **3des** | **aes128** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** }] | [**prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] | [**prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }]] * [**-ki** *aliveinterval* [**-kc** *alivecountmax*]] command to log in to another device.

- IPv6 mode:

  run the **stelnet ipv6** [**-a** *source-address*] *host-ipv6* [**-oi** *interface-type interface-number*] [*port-number*] [[**-vpn6-instance** *vpn-instance-name*] | [**prefer_kex** { **dh_group1** | **dh_exchange_group** }] | [**prefer_ctos_cipher** { **des** | **3des** | **aes128** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** }] | [**prefer_stoc_cipher** { **des** | **3des** | **aes128** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** }] | [**prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] | [**prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }]] * [**-ki** *aliveinterval* [**-kc** *alivecountmax*]] command to log in to another device.

When port 22 is specified as the protocol port number for the STelnet server, the STelnet client can log in with no port number specified. If another port number is specified as the protocol port number for the STelnet server, you must specify the port number used by the client to log in.

When configuring an STelnet client to log in to an SSH server, you can specify the source IP address, select a key exchange algorithm, an encryption algorithm, and an HMAC algorithm, and enable the keepalive function on the client.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

DES, 3DES, MD5, MD5_96, SHA1, and SHA1_96 encryption algorithm cannot ensure security. AES128, AES128-CTR, AES192-CTR or AES256-CTR encryption algorithm is recommended.

----End

Verifying the Configuration

- Run the **display ssh server** command to check the mapping between all SSH servers and RSA or ECC public keys on the SSH client

9.8 Configuring the Redirection Function for Device Login

After completing redirection configuration, you can log in to a remote serial port device from the local device to configure and manage the remote device.

Pre-configuration Tasks

Before logging in to a device through redirection, complete the following tasks:

- Start a remote device.
- Use a TTY user interface: ensuring that the remote device is directly connected to the 8AS card or 2SA card (8AS card is recommended) on the router using an asynchronous serial cable, and the physical and protocol status of the asynchronous serial interface on the router is Up.

  NOTE

  For details about the asynchronous serial cable, see "8AS Cable" or "Serial Cable (CON/RS232)" in the *Huawei AR Series Access Routers Get to Know the Product - Hardware Description - Cables*.

9.8.1 (Optional) Configuring an Authentication Mode for TTY User Interface

You can configure an authentication mode for TTY user interface to ensure secure login through the redirection function.

Context

The TTY user interface supports AAA authentication and password authentication.

- AAA authentication: Users must enter both user names and passwords for login. If either a user name or a password is incorrect, the login fails.
- Password authentication: Users must enter passwords for login. Only after a user enters the correct password does the device allow the users to log in.

Procedure

- Configure AAA authentication.

 Copyright © Huawei Technologies Co., Ltd.

a. Run **system-view**

The system view is displayed.

b. Run **user-interface tty** *tty-number*

The TTY user interface view is displayed.

c. Run **authentication-mode aaa**

The authentication mode is set to AAA authentication.

d. Run **quit**

Exit the Console or TTY user interface view.

e. Run **aaa**

The AAA view is displayed.

f. Run **local-user** *user-name* **password** { **cipher** | **irreversible-cipher** } *password*

A local user account is created and a password is configured.

g. Run **local-user** *user-name* **service-type telnet**

The access type of the local user is set to **Telnet**.

h. Run **quit**

Exit the AAA view.

- Configure password authentication.
  a. Run **system-view**

  The system view is displayed.

  b. Run **user-interface console 0**

  The console user interface view is displayed.

  Or run **user-interface tty** *tty-number*

  The TTY user interface view is displayed.

  c. Run **authentication-mode password**

  The authentication mode is set to password authentication.

  d. Run **set authentication password cipher**

  An authentication password is set.

----End

9.8.2 Logging In to a Device Through Redirection

This section describes how to configure the redirection function and use this function to log in to a remote device.

Context

To manage a remote device that can transmit data only through a serial port, configure the redirection function on the current device.

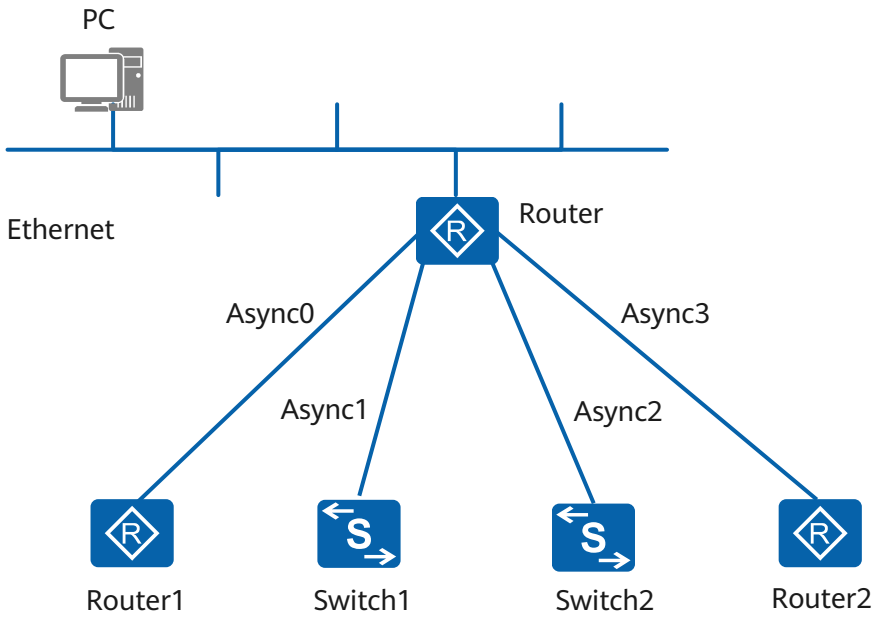
 Copyright © Huawei Technologies Co., Ltd.

A remote device can be a router, a switch, an electricity terminal, a finance terminal, or other terminals that use serial ports to transmit data.

- Managing remote routers and switches

  A device equipped with an 8AS card is used as an example. As shown in **Figure 9-9**, there are two routers and two switches connected to the device. The redirection function on the device can be used to manage remote devices that can only be managed through serial ports. The asynchronous serial port on the device is connected to the serial ports on the remote devices for users to manage and maintain the remote devices.

  Figure 9-9 Diagram for login through redirection (1)

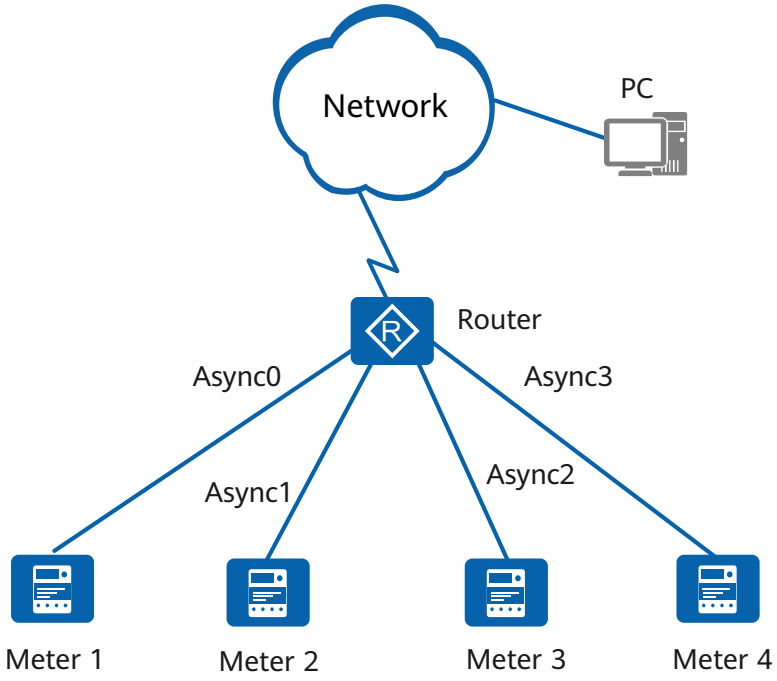


- Managing terminals such as intelligent electricity meters, intelligent water meters, and automatic teller machines

  As shown in **Figure 9-10**, the redirection function is enabled on the device. The device listens to the specified TCP port and receives data packets from the terminals through serial ports. After receiving data packets, the device encapsulates the packets into Ethernet frames so that they can be transmitted over an Ethernet network. This implements the remote data transmission and management on the terminals.

 Copyright © Huawei Technologies Co., Ltd.

Figure 9-10 Diagram for login through redirection (2)



Procedure

Step 1 Enable the redirection function on the router.

1. Run **system-view**

   The system view is displayed.
2. Run **interface async** *interface-number*

   The asynchronous interface view is displayed.
3. Run **async mode flow**

   The asynchronous serial interface is configured to work in flow mode.

   By default, an asynchronous serial interface works in protocol mode.
4. Run **quit**

   Exit from the asynchronous serial interface view.
5. Run:**user-interface tty** *tty-number*

   The TTY user interface view is displayed.

   When configuring the TTY user interface, pay attention to the following points:

   - After an 8AS interface card registers successfully, the device generates random numbers for TTY user interfaces. To view the TTY user interface number mapped to an asynchronous serial port, run the **display user-interface** command.
   - If the modem function is enabled on a TTY user interface, the redirection function does not take effect on the TTY user interface.

 Copyright © Huawei Technologies Co., Ltd.

6. (Optional) Run **authentication-mode** { **password** | **aaa** }

   A user authentication mode is specified.

   For details on configuration of the authentication mode, see **Configuring an Authentication Mode for the TTY User Interface**.

7. Run **redirect** [**ssh**] **enable**

   The redirection function is enabled.

   By default, the redirection function is disabled.

8. (Optional) Run **transparent-mode enable**

   The transparent transmission mode for redirection on the serial port is enabled.

   By default, the transparent transmission mode for redirection on a serial port is disabled.

   The device checks data redirected by a serial port and discards unidentifiable data, damaging the original data. You can run this command to ensure the original data integrity. The device will transparently transmit data without checking it.

9. Run **undo shell**

   The terminal service is disabled on the user interface.

   By default, the terminal service is disabled on a TTY user interface.

10. (Optional) Run **redirect binding vpn-instance** *vpn-instance-name*

    The redirection function is associated with a VPN instance.

    By default, the redirection function is not associated with any VPN instance, and all users on public and private networks can use the redirection function to log in to remote devices.

11. (Optional) Run **redirect** [**ssh**] **listen-port** *port-number*

    A port number is specified for setting up connections through the redirection function.

    By default, the port number that the local device uses to set up a connection with a remote device is 2000 plus *tty-number*. When the default port number is used by another service, perform this step to set a new port number.

Step 2 Log in to a device from a terminal through redirection.

- Telnet mode

  Log in to a device from a terminal through redirection in Telnet mode. The Windows command line is used as an example.

  a. Open the command line window.

  b. Run the **telnet** *host-name port-number* command to log in to the device through redirection.

     In the command, *host-name* is the IP address or host name of the router with the redirection function enabled, and *port-number* is the default listening port number (2000 plus *tty-number*) or the port number configured using the **redirect listen-port** command. (The following information is only for reference.)

 Copyright © Huawei Technologies Co., Ltd.

```
C:\Documents and Settings\Administrator> telnet 10.1.1.1 2042
Press CTRL_] to quit telnet mode
  Trying 10.1.1.1...
  Connected to 10.1.1.1...
Login authentication

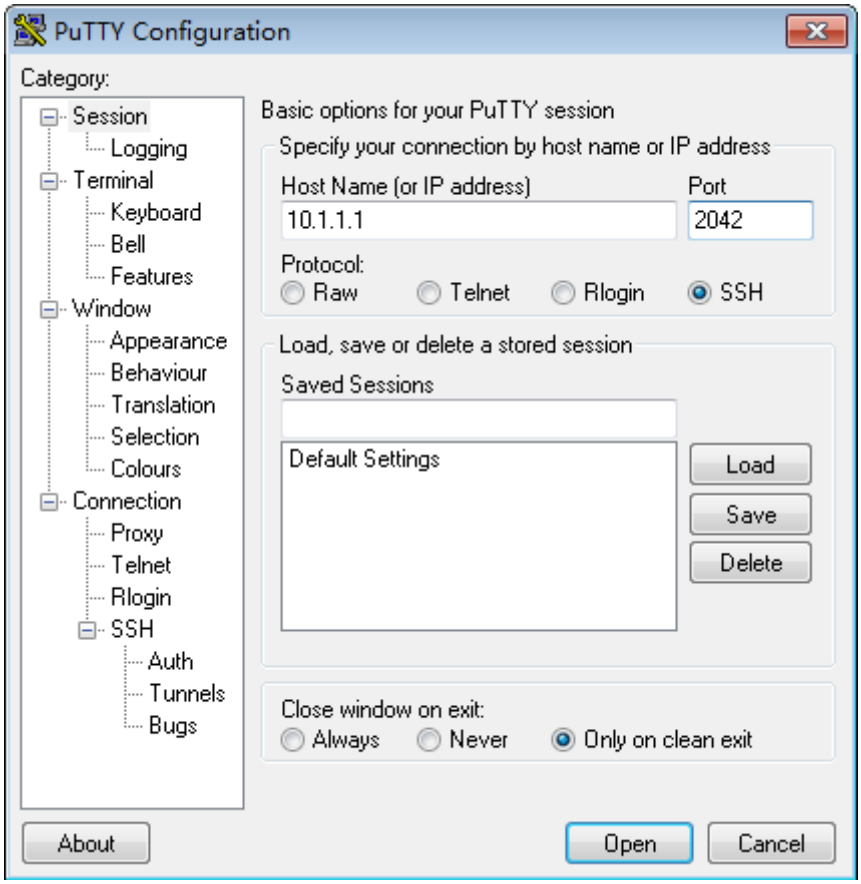

Password:
 <Router>
```

- STelnet mode

  Log in to a device from a terminal through redirection in STelnet mode. The third-party software PuTTY is used as an example.

  # Log in to the device using PuTTY. Set the protocol type to SSH, **Host Name** to the IP address or host name of the redirection-enabled router, and **Port** to the default port number (2000 plus TTY number) or the port number specified using the **redirect ssh listen-port** command. (The following information is only for reference.)

  Figure 9-11 Using Putty to redirect to a device in STelnet mode



  # Click **Open**. Enter the user name and password at the prompt, and press **Enter**. You have logged in to the device. (The following information is only for reference.)

```
login as: client001
client001@10.1.1.1's password:
```

 Copyright © Huawei Technologies Co., Ltd.

```
<Router>
```

----End

Verifying the Configuration

Run the **display tcp status** command to check the current TCP connection status.

9.9 Configuring Reverse Telnet Login

The reverse Telnet function enables dumb terminals that are directly connected to a router using asynchronous serial cables or console cables to log in to a remote server.

Pre-configuration Tasks

Before logging in to a device through reverse Telnet, complete the following tasks:

- Start a remote device.
- Use a TTY user interface: ensuring that a dumb terminal is directly connected to the 1SA or 2SA card of the router with an asynchronous cable and the physical status and protocol status of the connected asynchronous interface are Up.
- Use the console user interface: ensuring that the remote device is directly connected to the console interface on the router.
- Ensure that there are reachable routes between the router and the remote server.

NOTE

For details about the asynchronous serial cable, see "SA Cable" in the *Huawei AR Series Access Routers Get to Know the Product - Hardware Description - Cables*.

9.9.1 Configuring an Authentication Mode for the Console or TTY User Interface

You can configure an authentication mode for the console user interface or a TTY user interface to ensure secure login through the reverse Telnet function.

Context

The console or TTY user interface supports AAA authentication and password authentication.

- AAA authentication: Users must enter both user names and passwords for login. If either a user name or a password is incorrect, the login fails.
- Password authentication: Users must enter passwords for login. Only after a user enters the correct password does the device allow the users to log in.

Procedure

- Configure AAA authentication.

 Copyright © Huawei Technologies Co., Ltd.

a. Run **system-view**

The system view is displayed.

b. Run **user-interface tty** *tty-number*

The TTY user interface view is displayed.

c. Run **authentication-mode aaa**

The authentication mode is set to AAA authentication.

d. Run **quit**

Exit the Console or TTY user interface view.

e. Run **aaa**

The AAA view is displayed.

f. Run **local-user** *user-name* **password** { **cipher** | **irreversible-cipher** } *password*

A local user account is created and a password is configured.

g. Run **local-user** *user-name* **service-type telnet**

The access type of the local user is set to **Telnet**.

h. Run **quit**

Exit the AAA view.

- Configure password authentication.

a. Run **system-view**

The system view is displayed.

b. Run **user-interface console 0**

The console user interface view is displayed.

Or run **user-interface tty** *tty-number*

The TTY user interface view is displayed.

c. Run **authentication-mode password**

The authentication mode is set to password authentication.

d. Run **set authentication password cipher**

An authentication password is set.

----End

9.9.2 Logging In to a Device Through Reverse Telnet (Direct Connection Through an Asynchronous Cable)

This section describes how to configure reverse Telnet and use this function to log in to a device through an asynchronous cable.

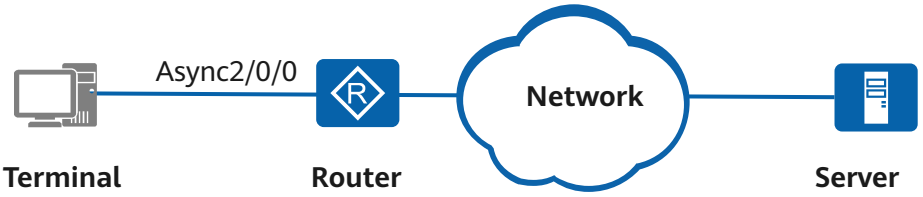
Context

As shown in **Figure 9-12**, a multimedia software terminal (dumb terminal) is connected to the router with an asynchronous cable, and the router is connected

 Copyright © Huawei Technologies Co., Ltd.

to a server. The terminal cannot communicate with the server directly. To enable the dumb terminal to communicate with the server, you can configure reverse Telnet on the router. The router then acts as a client to transmit data from the terminal to the server.

Figure 9-12 Diagram for login through reverse Telnet



Procedure

Step 1 Run **system-view**

The system view is displayed.

Step 2 Run **interface async** *interface-number*

The asynchronous serial interface view is displayed.

Step 3 Run **async mode flow**

The asynchronous serial interface is configured to work in flow mode.

By default, an asynchronous serial interface works in protocol mode.

Step 4 Run **quit**

Exit from the asynchronous serial interface view.

Step 5 Run **user-interface tty** *tty-number*

The TTY user interface view is displayed.

After a 1SA, or a 2SA interface card registers successfully, the device generates random numbers for TTY user interfaces. To view the TTY user interface number mapped to an asynchronous serial port, run the **display user-interface** command.

NOTE

If the modem function is enabled on a TTY user interface, the reverse Telnet function does not take effect on the TTY user interface.

Step 6 Run **undo shell**

The terminal service is disabled on the user interface.

By default, the terminal service is disabled on a TTY user interface.

Step 7 Run **connect** *host* [*port-number*] [**-a** *source-ip-address* | **-i** *interface-type interface-number*] [**-t** *interval*]

Configure connection parameters on the router to enable the dumb terminal to set up a connection with the remote server through the router.

By default, a dumb terminal cannot set up a connection with a remote server.

 Copyright © Huawei Technologies Co., Ltd.

Step 8 (Optional) Run **exline-breaker enable**

The router is enabled to add line breakers in output information.

By default, the function of adding a line break is disabled.

To configure the calling end to add line break **\n** when sending carriage return line break **\r\n** so that the calling and called ends have the same data, perform this step to enable the function of adding a line break.

Step 9 Connect the dumb terminal to the router using an asynchronous cable and log in to the remote server from the terminal.

----End

Verifying the Configuration

Run the **display tcp status** command to check the current TCP connection status.

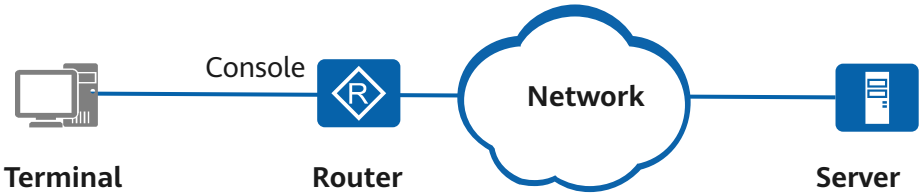
9.9.3 Configuring Reverse Telnet Login (Direct Connection Through a Console Cable)

This section describes how to configure reverse Telnet and use this function to log in to a device through a console cable.

Context

As shown in **Figure 9-13**, a multimedia software terminal (dumb terminal) is connected to the console interface of the router through a console cable, and the router is connected to a server. The terminal cannot communicate with the server directly. To enable the dumb terminal to communicate with the server, you can configure reverse Telnet on the router. The router then acts as a client to transmit data from the terminal to the server.

Figure 9-13 Networking for login through reverse Telnet



Procedure

Step 1 Run **system-view**

The system view is displayed.

Step 2 Run **user-interface console 0**

The console user interface view is displayed.

Step 3 Run **connect** *host* [*port-number*] [**-a** *source-ip-address* | **-i** *interface-type interface-number*] [**-t** *interval*]

 Copyright © Huawei Technologies Co., Ltd.

The dumb terminal is configured to set up a connection with the remote server through the router.

By default, a dumb terminal cannot set up a connection with a remote server.

Step 4 (Optional) Run **exline-breaker enable**

The function of adding a line break is enabled.

By default, the function of adding a line break is disabled.

To configure the calling end to add line break **\n** when sending carriage return line break **\r\n** so that the calling and called ends have the same data, perform this step to enable the function of adding a line break.

Step 5 Run **undo shell**

The terminal service is disabled on the console user interface.

By default, the terminal service is enabled on the console user interface.

NOTE

For the device with the Config button, you can also press and hold down the config button for less than 5s, the terminal service on the console user interface will be switched between **shell** and **undo shell** once.

Step 6 Connect the dumb terminal to the console interface of the router using a console cable and log in to the remote server from the terminal.

----End

Verifying the Configuration

Run the **display tcp status** command to check the current TCP connection status.

9.10 Typical Operations After Login

After logging in to a device through a console port or mini USB port, or using Telnet or STelnet, you can perform service configurations and the following common operations on the device.

Displaying Online Users

After logging in to a device, you can view user login information of each user interface.

Run the **display users** [**all**] command to view the user login information of user interfaces.

Setting an Authentication Password for Switching User Levels

NOTE

AR3200 series routers do not support this function in active/standby switchover scenarios.

Users at a higher level can set an authentication password used to switch a user from a lower level to a higher level. If a user wants to use a command whose level

 Copyright © Huawei Technologies Co., Ltd.

is higher than the user level, the user can use the authentication password to switch to the higher level.

1. Run the **system-view** command to enter the system view.
2. Run the **super password** [**level** *user-level*] **cipher** command to set an authentication password used to switch a user from a lower level to a higher level.

Switching User Levels

NOTE

AR3200 series routers do not support this function in active/standby switchover scenarios.

You need to enter a password when switching from a low user level to a higher one.

1. Run the **super** [*level*] command in the user view to switch the user level.

   NOTE

   If the entered target user level is lower than or equal to the current user level, the system directly sets the entered user level as the target user level, and displays a message. If the target level is higher than the current user level, the system asks the user to enter the authentication password.

2. Enter the password as prompted.

   If the password is correct, you will switch to a higher user level. If you enter an incorrect password three times consecutively, the system returns to the user view and the user level remains unchanged.

Sending Messages to Other User Interfaces

You can send messages from the current user interface to other user interfaces.

1. Run the **send** { **all** | *ui-number* | *ui-type ui-number1* } command to enable message exchange between user interfaces.
2. Enter the message to send as prompted. Press **Ctrl+Z** or **Enter** to end message input and press **Ctrl+C** to end the current operation.
3. At the system prompt, choose **Y** to send the message and **N** to cancel message sending.

Automatically Searching for the undo Command in the Upper-level View

When you run the undo command not registered with the current view, the system returns to the upper-level view to search for this undo command. If the undo command can be found, it takes effect. If the undo command cannot be found, the system continues to search for it in the next upper-level view until the system view.

1. Run the **system-view** command to display the system view.
2. Run the **matched upper-view** command to enable the undo command to run in the upper-level view.

   By default, the undo command does not automatically match the upper-level view.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The **matched upper-view** command is only valid for current login users who run this command.

You are not advised to configure the undo command to automatically match the upper-level view, unless necessary.

Locking a User Interface

When you need to temporarily leave the operation terminal, lock the user interface to prevent unauthorized users from operating the terminal.

1. Run the **lock** command to lock the user interface.
2. Enter the lock password and confirm password as prompted.

```
<Huawei> lock
Enter Password(<8-128>):
Confirm Password:
Info: The terminal is locked.
```

After you run the **lock** command, the system prompts you to enter the lock password and confirm password. If the two passwords are the same, the current interface is locked successfully.

To unlock the user interface, you must press **Enter** and enter the correct login password as prompted.

9.11 Configuration Examples for CLI Login

This section describes examples of logging in to a device through a console port, Telnet, or STelnet.

9.11.1 Example for Logging In to the Device Through a Console Port

Networking Requirements

If a user cannot remotely log in to a device, the user will attempt to log in through the console port. By default, a user only needs to pass password authentication to log in to the device from the console user interface. To prevent unauthorized users from accessing the device, change the authentication mode of the console user interface to AAA authentication.

Figure 9-14 Networking diagram of user login through a console port



Configuration Roadmap

The configuration roadmap is as follows:

 Copyright © Huawei Technologies Co., Ltd.

1. Use the terminal simulation software to log in to the device through a console port.
2. Configure the authentication mode of the console user interface.

NOTE

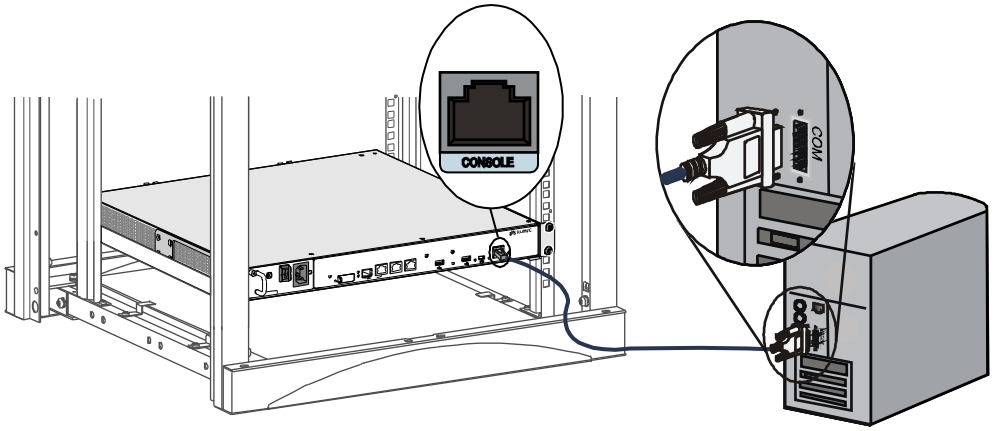
You can use the built-in terminal emulation software (such as the PuTTY) on the PC. If no built-in terminal emulation software is available, use the third-party terminal emulation software. For details, see the software user guide or online help.

Procedure

Step 1 Use the terminal simulation software to log in to the device through a console port.

1. Insert the DB9 connector of the console cable delivered with the product to the 9-pin serial port on the PC, and insert the RJ45 connector to the console port of the device, as shown in **Figure 9-15**.

Figure 9-15 Connecting to the device through the console port



2. Start the terminal emulation software on the PC. Create a connection, select the connected port, and set communication parameters.

NOTE

A PC may have multiple connection interfaces; therefore, the interface connected through the console cable is selected in this example. Generally, COM1 is selected.

If the serial port communication parameters of the device are modified, modify the communication parameters on the PC accordingly (ensure that the parameter values are the same) and re-establish the connection.

3. Press **Enter** until the system prompts you to enter the password. (The system will prompt you to enter the user name and password in AAA authentication. The following information is only for reference.)

```
Login authentication


Password:
```

You can run commands to configure the device. Enter a question mark (?) whenever you need help.

 Copyright © Huawei Technologies Co., Ltd.

Step 2 Configure the authentication mode of the console user interface.

```
<Huawei> system-view
<Huawei> sysname Router
[Router] user-interface console 0
[Router-ui-console0] authentication-mode aaa
[Router-ui-console0] user privilege level 15
[Router-ui-console0] quit
[Router] aaa
[Router-aaa] local-user admin1234 password irreversible-cipher Helloworld@6789
[Router-aaa] local-user admin1234 privilege level 3
[Router-aaa] local-user admin1234 service-type terminal
```

After the preceding operations, you can re-log in to the device on the console user interface only by entering the user name **admin1234** and password **Helloworld@6789**.

----End

Configuration Files

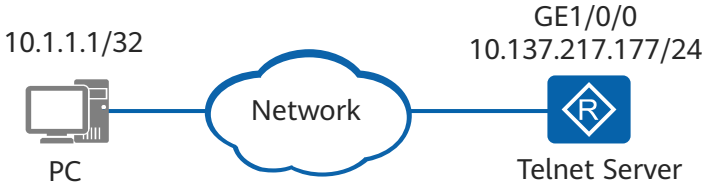
```
#
sysname Router
#
aaa
 local-user admin1234 password irreversible-cipher %@%@HW=5%Mr;:2)/RX$FnU1HLO%-TBMp4wn%;~\#
%iAut}_~O%0L%@%@
 local-user admin1234 privilege level 3
 local-user admin1234 service-type terminal
#
user-interface con 0
 authentication-mode aaa
#
return
```

9.11.2 Example for Configuring a Security Policy to Limit Telnet Login

Networking Requirements

As shown in **Figure 9-16**, the PC and the server (Huawei device) are reachable to each other. To implement easy remote configuration and management of the device, configure AAA authentication for Telnet users on the server and configure an ACL security policy that allows only users in compliance with the security policy to log in to the device.

Figure 9-16 Networking diagram for Configuring a Security Policy to Limit Telnet Login



 Copyright © Huawei Technologies Co., Ltd.

NOTE

The Telnet protocol poses a security risk, and therefore the STelnet V2 protocol is recommended.

Configuration Roadmap

The following configurations are performed on the Router. The configuration roadmap is as follows:

1. Configure the Telnet login mode to implement remote network device maintenance.
2. Configure an ACL security policy to ensure that only users in compliance with the security policy can log in to the device.
3. Configure the administrator's user name and password and the AAA authentication mode to ensure that only users passing the authentication can log in to the device.

Procedure

Step 1 Set the server listening port number and enable the server function.

```
<Huawei> system-view
[Huawei] sysname Telnet Server
[Telnet Server] telnet server enable
[Telnet Server] telnet server port 1025
```

Step 2 Set the VTY user interface parameters.

Set the maximum number of VTY user interfaces.

```
[Telnet Server] user-interface maximum-vty 8
```

Set the IP address of the device to which the user is allowed to log in.

```
[Telnet Server] acl 2001
[Telnet Server-acl-basic-2001] rule permit source 10.1.1.1 0
[Telnet Server-acl-basic-2001] quit
[Telnet Server] user-interface vty 0 7
[Telnet Server-ui-vty0-7] acl 2001 inbound
```

Configure the terminal attributes of the VTY user interface.

```
[Telnet Server-ui-vty0-7] shell
[Telnet Server-ui-vty0-7] idle-timeout 20
[Telnet Server-ui-vty0-7] screen-length 30
[Telnet Server-ui-vty0-7] history-command max-size 20
```

Configure the user authentication mode of the VTY user interface.

```
[Telnet Server-ui-vty0-7] authentication-mode aaa
[Telnet Server-ui-vty0-7] quit
```

Step 3 Configure the login user information.

Configure the login authentication mode.

```
[Telnet Server] aaa
[Telnet Server-aaa] local-user admin1234 password irreversible-cipher Helloworld@6789
[Telnet Server-aaa] local-user admin1234 service-type telnet
[Telnet Server-aaa] local-user admin1234 privilege level 3
[Telnet Server-aaa] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Step 4 Configure the client login.

Enter commands at the command line prompt to log in to the device through Telnet.

```
C:\Documents and Settings\Administrator> telnet 10.137.217.177 1025
```

Press **Enter**, and enter the user name and password in the login window. If the authentication is successful, the command line prompt of the user view is displayed. The user view configuration environment is displayed.

```
Login authentication

Username:admin1234
Password:
<Telnet Server>
```

----End

Configuration Files

Telnet server configuration file

```
#
 sysname Telnet Server
#
acl number 2001
 rule 5 permit source 10.1.1.1 0
#
aaa
 local-user admin1234 password irreversible-cipher %^%#*~Br";[g6Pv5Zf>$~{hY+N!`{$<[Y{;l02P)B,EBz\1FN!c
+%^%#
 local-user admin1234 privilege level 3
 local-user admin1234 service-type telnet
#
 telnet server enable
 telnet server port 1025
#
user-interface maximum-vty 8
user-interface vty 0 7
 acl 2001 inbound
 authentication-mode aaa
 history-command max-size 20
 idle-timeout 20 0
 screen-length 30
#
return
```

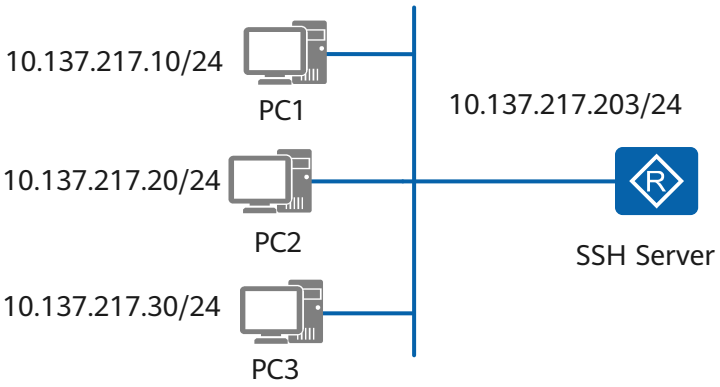
9.11.3 Example for Logging In to the Device Through STelnet

Networking Requirements

As shown in **Figure 9-17**, users require secure remote login, but Telnet cannot provide a secure authentication method. In this scenario, STelnet can be configured to ensure security of remote login. PC1 and PC2 have reachable routes to the SSH server, and 10.137.217.203 is the IP address of the management interface on the SSH server. Two login users client001 and client002 need to be configured on the SSH server. PC1 uses the account of client001 to log in to the SSH server through password authentication; PC2 uses the account of client002 to log in to the SSH server through RSA authentication. Configure a security policy to ensure that only PC1 and PC2 can be used to log in to the device.

 Copyright © Huawei Technologies Co., Ltd.

Figure 9-17 Networking diagram of logging in to the device through STelnet



NOTE

The STelnet V1 protocol poses a security risk, and therefore the STelnet V2 mode is recommended.

Configuration Roadmap

The configuration roadmap is as follows:

1. Install the SSH server software on PC1. Install the key pair generation software, public key conversion software, and SSH server login software on PC2.
2. Generate a local key pair on the SSH server to implement secure data exchange between the server and client.
3. Configure different authentication modes for the SSH users **client001** and **client002** on the SSH server.
4. Enable the STelnet service on the SSH server.
5. Configure a security policy to ensure that only PC1 and PC2 can be used to log in to the device.
6. Configure the STelnet server type for the SSH users **client001** and **client002** on the SSH server.
7. Log in to the SSH server as the **client001** and **client002** users through STelnet.

Procedure

Step 1 Generate a local key pair on the server.

```
<Huawei> system-view
[Huawei] sysname SSH Server
[SSH Server] rsa local-key-pair create
The key name will be: Host
RSA keys defined for Host already exist.
Confirm to replace them? (y/n):y
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is less than 2048,
       It will introduce potential security risks.
Input the bits in the modulus[default = 2048]:2048
Generating keys...
```

 Copyright © Huawei Technologies Co., Ltd.

```
.....+++
....+++
.....++++++++
.............++++++++
```

Step 2 Create an SSH user on the server.

Configure the VTY user interface.

```
[SSH Server] user-interface vty 0 4
[SSH Server-ui-vty0-4] authentication-mode aaa
[SSH Server-ui-vty0-4] protocol inbound ssh
[SSH Server-ui-vty0-4] quit
```

- Create an SSH user named **client001**.

  # Create an SSH user named **client001** and configure the password authentication mode for the user.

  ```
  [SSH Server] aaa
  [SSH Server-aaa] local-user client001 password irreversible-cipher Huawei@123
  [SSH Server-aaa] local-user client001 privilege level 3
  [SSH Server-aaa] local-user client001 service-type ssh
  [SSH Server-aaa] quit
  [SSH Server] ssh user client001 authentication-type password
  ```

- Create an SSH user named **client002**.

  # Create an SSH user named **client002** and configure the RSA authentication mode for the user.

  ```
  [SSH Server] aaa
  [SSH Server-aaa] local-user client002 password irreversible-cipher Helloworld@6789
  [SSH Server-aaa] local-user client002 privilege level 3
  [SSH Server-aaa] local-user client002 service-type ssh
  [SSH Server-aaa] quit
  [SSH Server] ssh user client002 authentication-type rsa
  ```

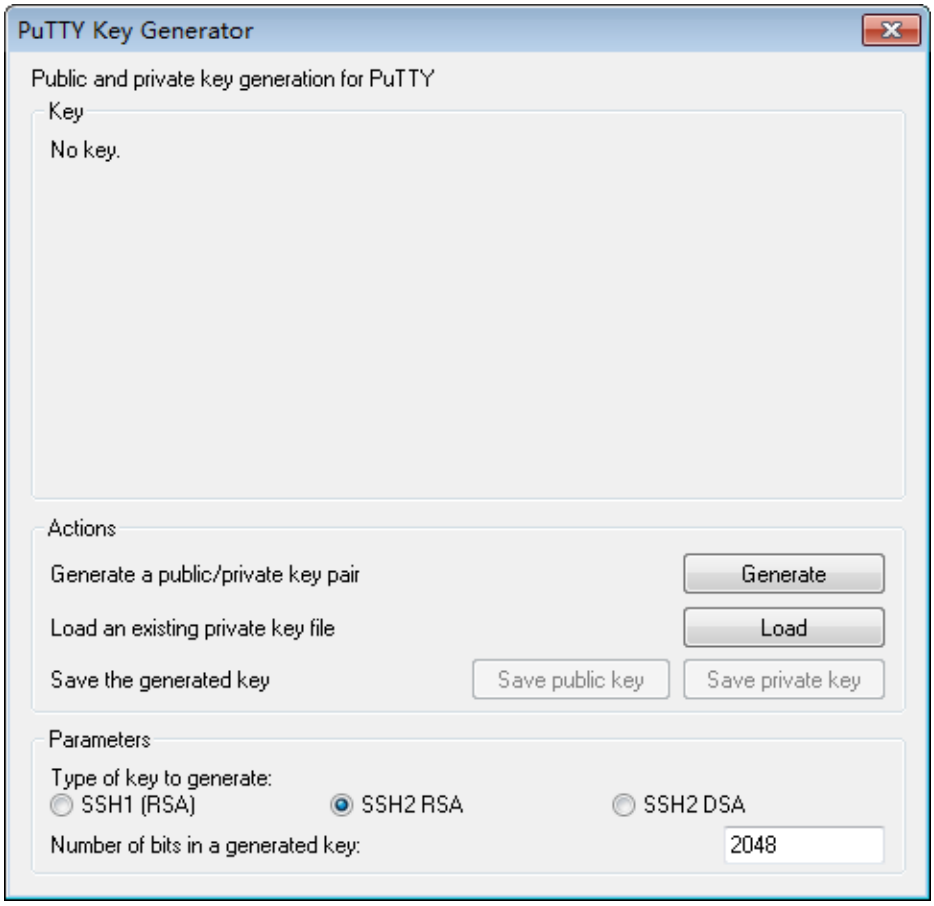
  # Generate a local key pair of the client on PC2.

  a. Run **puttygen.exe** on the client. It is used to generate the public and private key files.

     Select **SSH2 RSA** and click **Generate**. By moving the cursor in the blank area to generated the key.

 Copyright © Huawei Technologies Co., Ltd.

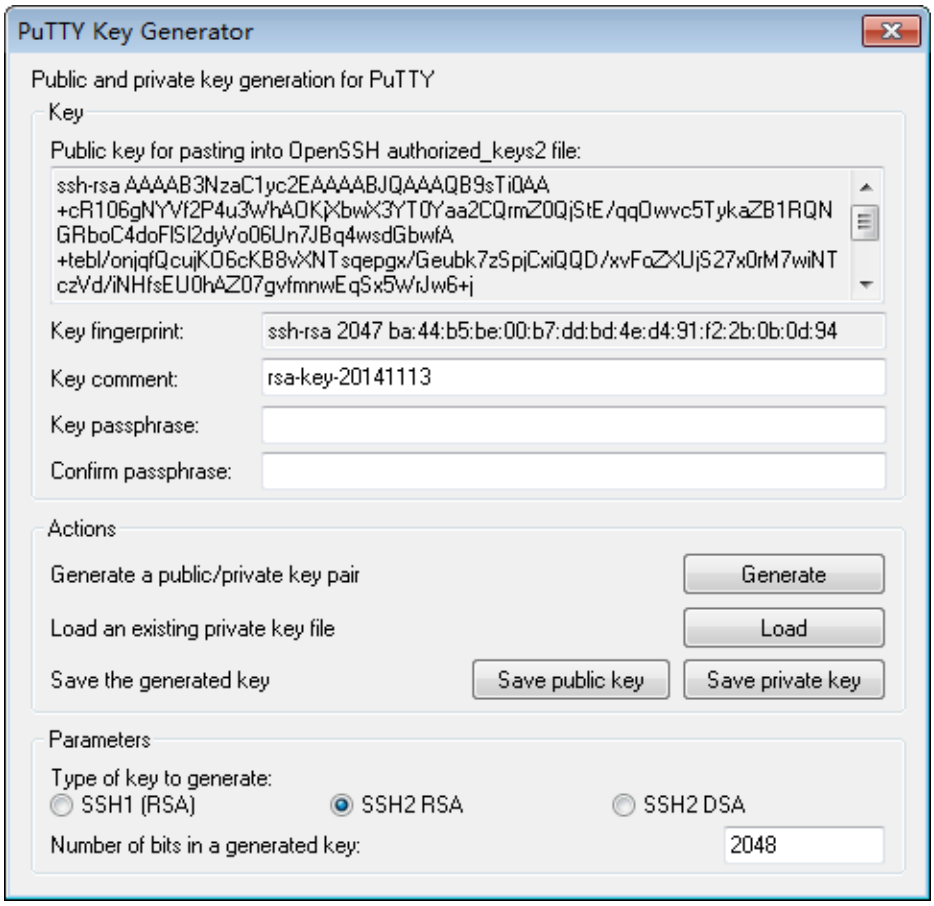
Figure 9-18 PuTTY Key Generate page (1)



After the key is generated, click **Save public key** to save the key in the **key.pub** file.

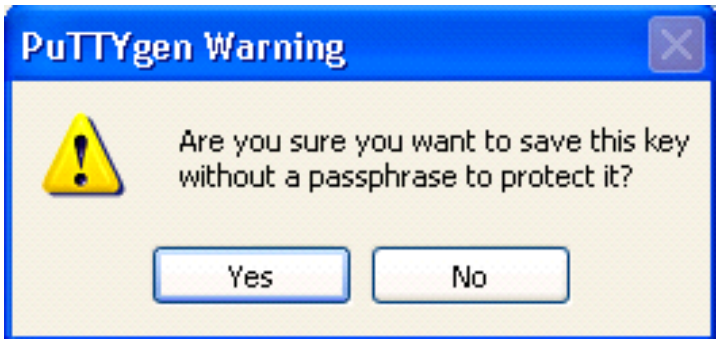
 Copyright © Huawei Technologies Co., Ltd.

Figure 9-19 PuTTY Key Generate page (2)



Click **Save private key**. The **PuTTYgen Warning** dialog box is displayed. Click **Yes**. The private key is saved in the **private.ppk** file.

Figure 9-20 PuTTY Key Generate page (3)

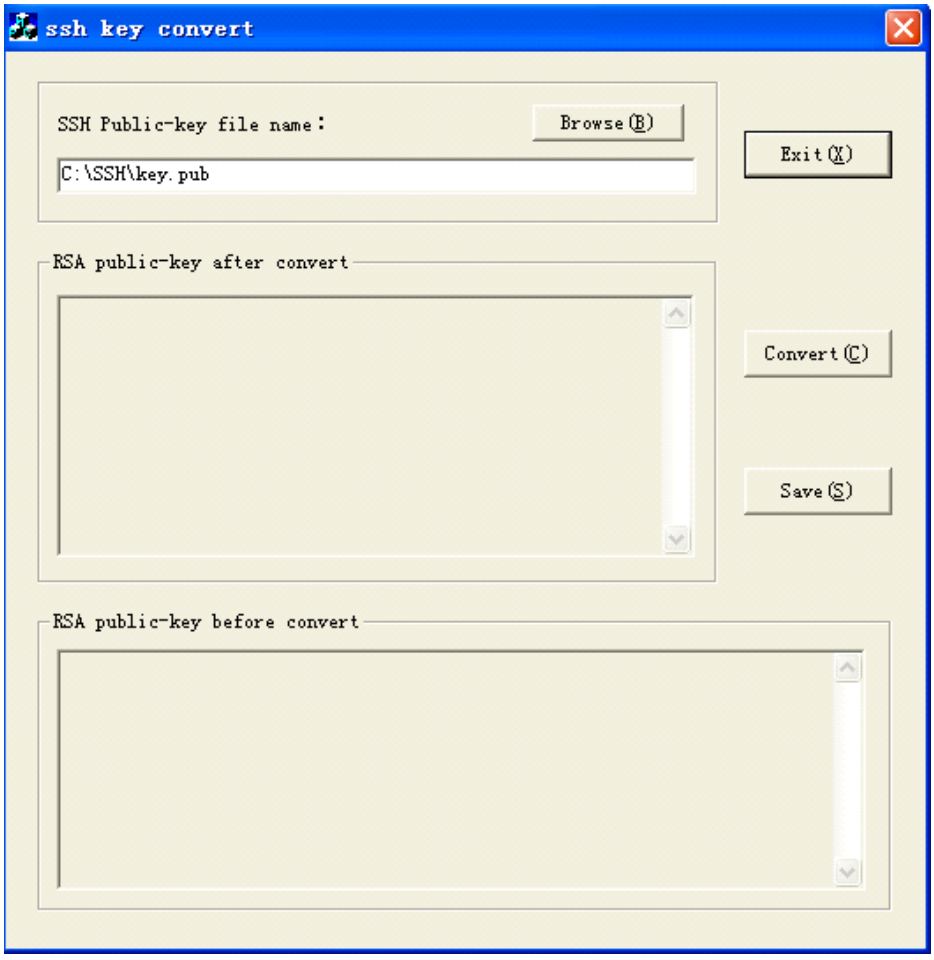


b. Run **sshkey.exe** on the client. Convert the generated public key to the character string required for the device.

   Open the **key.pub** file required by SSH that is generated in the previous step.

 Copyright © Huawei Technologies Co., Ltd.

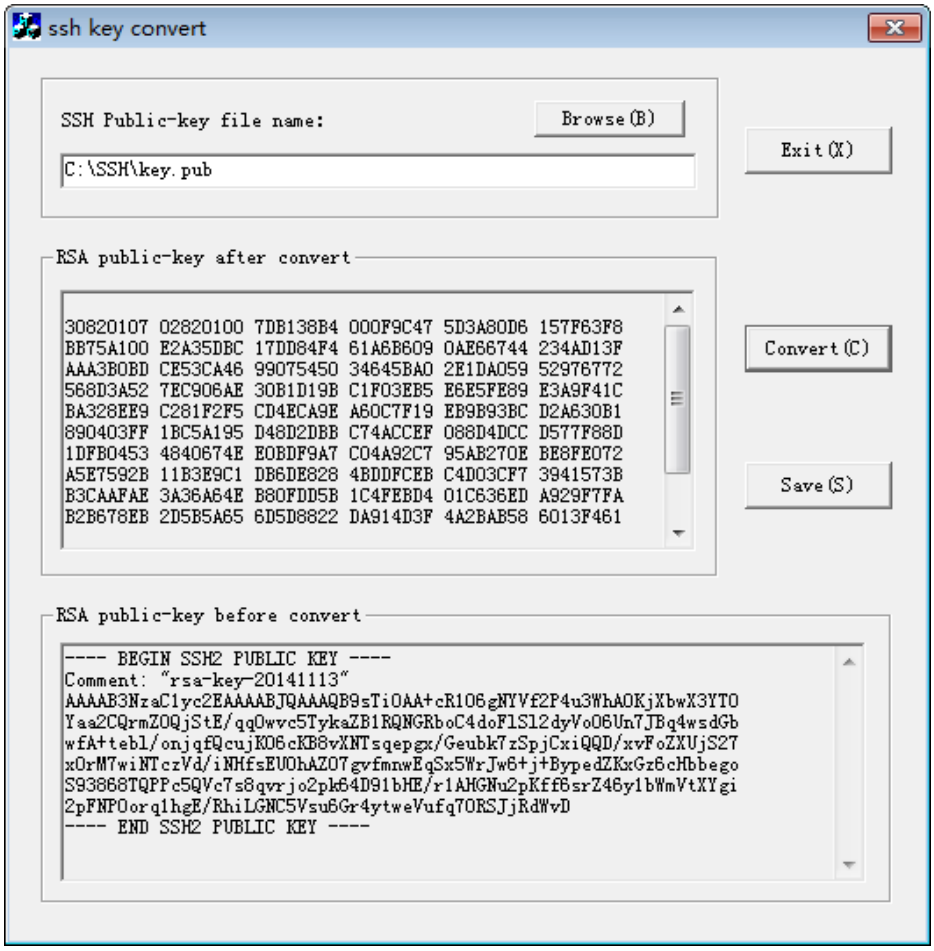
Figure 9-21 ssh key converter page (1)



Click **Convert(C)**. You can see the public keys before and after conversion.

 Copyright © Huawei Technologies Co., Ltd.

Figure 9-22 ssh key converter page (2)



Enter the RSA public key generated on PC2 to the SSH server.

```
[SSH Server] rsa peer-public-key rsakey001
[SSH Server-rsa-public-key] public-key-code begin
[SSH Server-rsa-key-code] 30820108 02820101 00DD8904 1A5E30AA 976F384B 5DB366A7
[SSH Server-rsa-key-code] 048C0E79 06EC6B08 8BB9567D 75914B5B 4EA7B2E5 1938D118
[SSH Server-rsa-key-code] 4B863A38 BA7E0F0D BE5C5AE4 CA55B192 B531AC48 B07D21E3
[SSH Server-rsa-key-code] 62E3F2A5 8C04C443 CF51CF51 136B5B9E 812AB1B7 1250EB24
[SSH Server-rsa-key-code] A4AE5083 A1DB18EC E2395C9B B806E8F0 0BE24FB5 16958784
[SSH Server-rsa-key-code] 403B617F 8AAAB1F8 C6DE8C3C F09E4D23 7D1C17BF 4AAF09C4
[SSH Server-rsa-key-code] 74C083AF 17CD3075 3396B322 32C57FF0 B1991971 02F1033B
[SSH Server-rsa-key-code] 81AA6D47 44520F23 685FAF72 04BA4B6E 615EF224 14E64E2A
[SSH Server-rsa-key-code] 331EEB7F 188D9805 96DBFD30 0C947A5A BA879DC4 F848B769
[SSH Server-rsa-key-code] 513C35CD B52B2917 02B77693 F79910EE 5287F252 977F985E
[SSH Server-rsa-key-code] 5F186C94 93F26780 4E7F5F9D 5287350A 0A4F4988 1BF6AB7C
[SSH Server-rsa-key-code] 1B020125
[SSH Server-rsa-key-code] public-key-code end
[SSH Server-rsa-public-key] peer-public-key end
```

Bind the RSA public key of the STelnet client to the SSH user client002 on the SSH server.

```
[SSH Server] ssh user client002 assign rsa-key rsakey001
```

Step 3 Enable the STelnet service on the SSH server.

Enable the STelnet service.

```
[SSH Server] stelnet server enable
```

 Copyright © Huawei Technologies Co., Ltd.

Step 4 Configure a security policy to ensure that only PC1 and PC2 can be used to log in to the device.

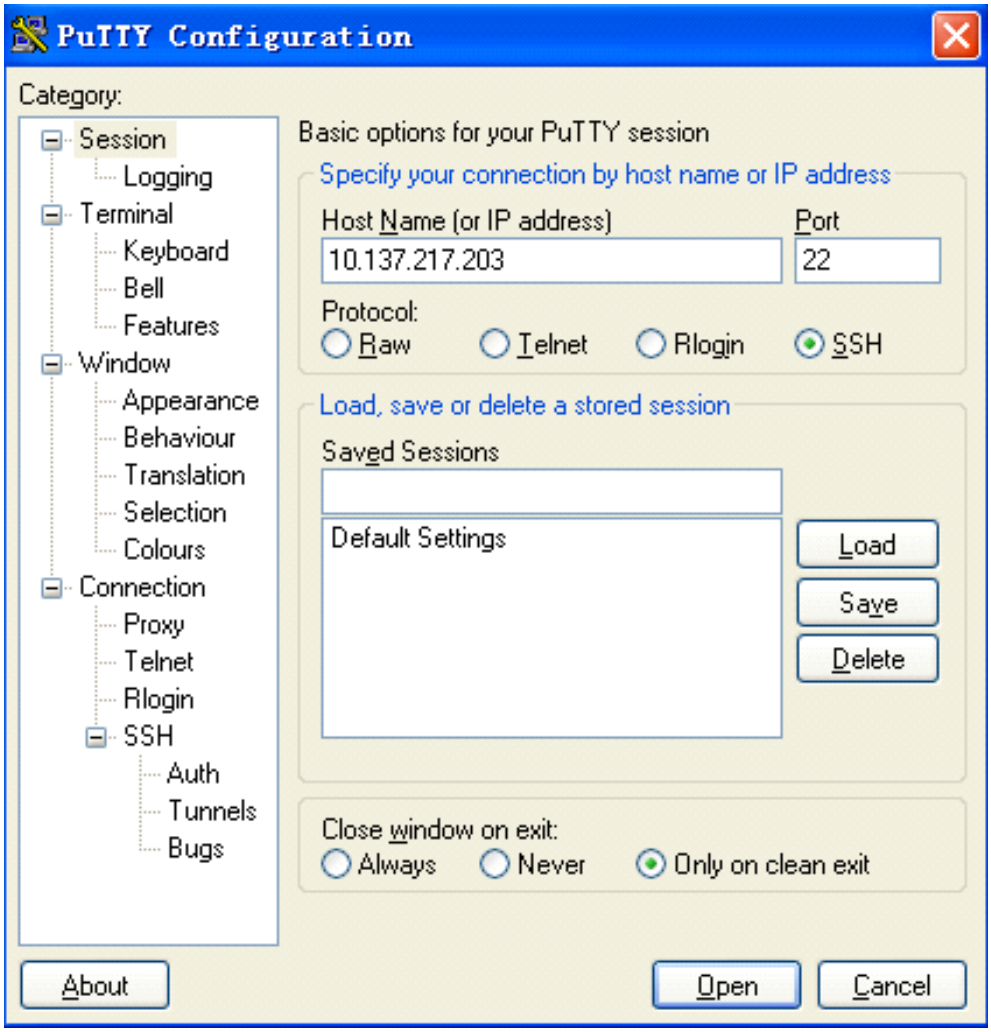
```
[SSH Server] acl 2001
[SSH Server-acl-basic-2001] rule permit source 10.137.217.10 0
[SSH Server-acl-basic-2001] rule permit source 10.137.217.20 0
[SSH Server-acl-basic-2001] rule deny source 10.137.217.30 0
[SSH Server-acl-basic-2001] quit
[SSH Server] user-interface vty 0 4
[SSH Server-ui-vty0-4] acl 2001 inbound
[SSH Server-ui-vty0-4] quit
```

Step 5 Verify the configuration.

- Log in to the SSH server as the **client001** user from PC1 using the password authentication mode.

  # Use the PuTTY software to log in to the device, enter the device IP address, and select the SSH protocol type.

  Figure 9-23 PuTTY Configuration page - password authentication mode



  # Click **Open**. Enter the user name and password at the prompt, and press **Enter**. You have logged in to the SSH server.

 Copyright © Huawei Technologies Co., Ltd.

```
login as: client001
Sent username "client001"

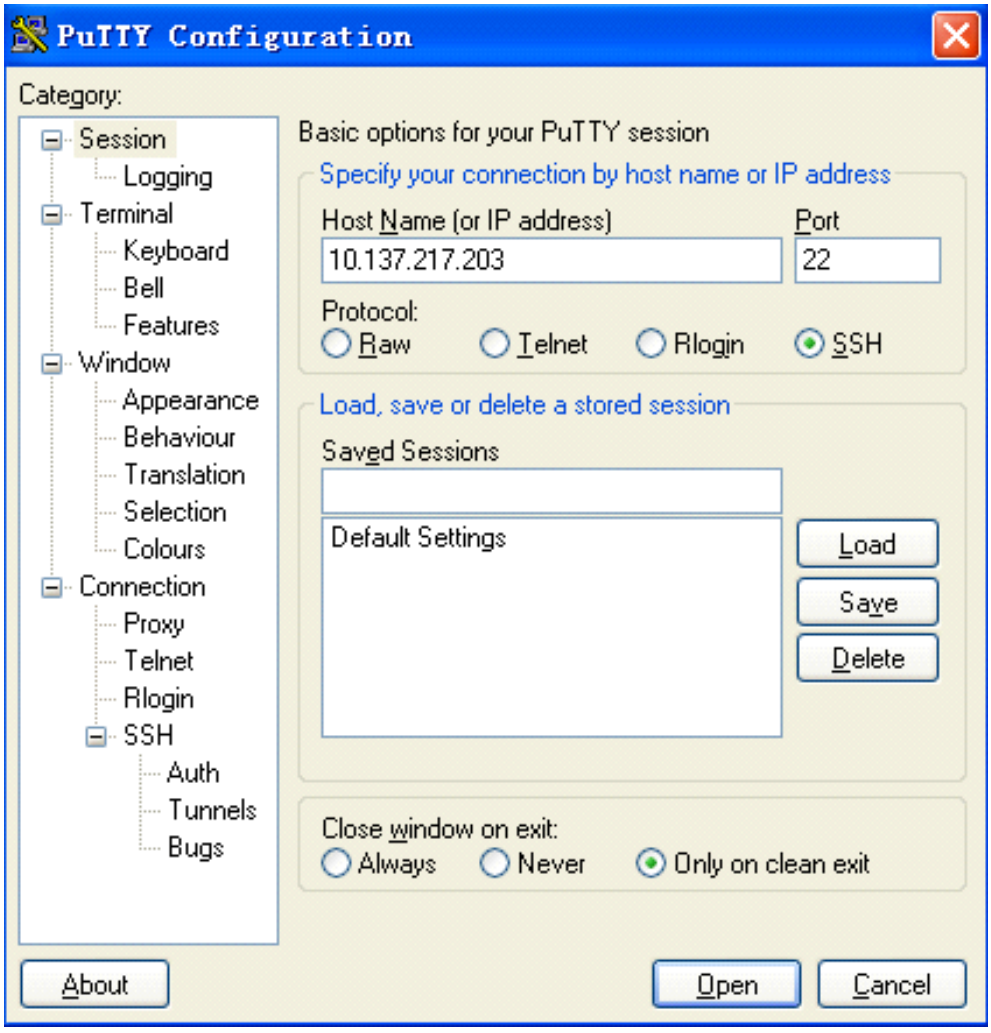
client001@10.137.217.203's password:

<SSH Server>
```

- Log in to the SSH server as the **client002** user from PC2 using the RSA authentication mode.

  # Use the PuTTY software to log in to the device, enter the device IP address, and select the SSH protocol type.

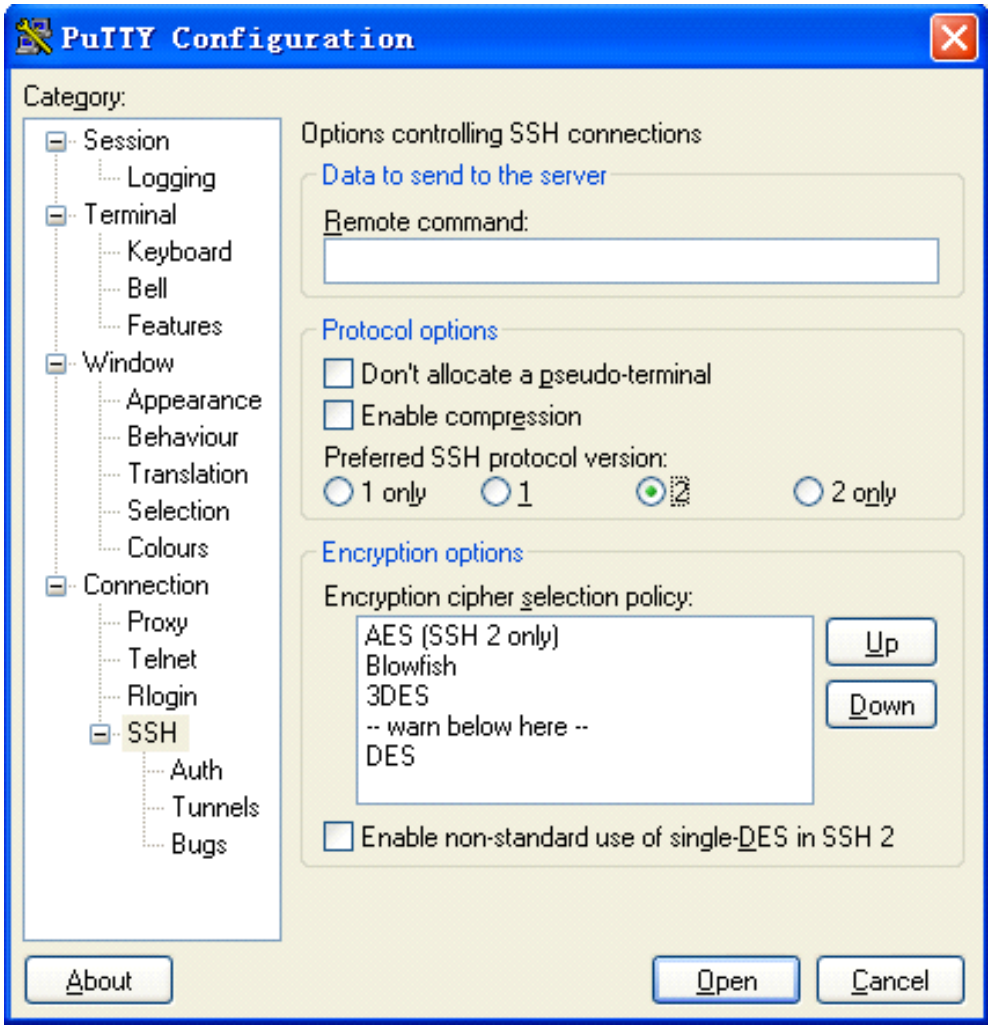
  Figure 9-24 PuTTY Configuration page - RSA authentication mode (1)



  # Choose **Connection** > **SSH** in the navigation tree. The page shown in **Figure 9-25** is displayed. Select **2** for **Preferred SSH protocol version**

 Copyright © Huawei Technologies Co., Ltd.

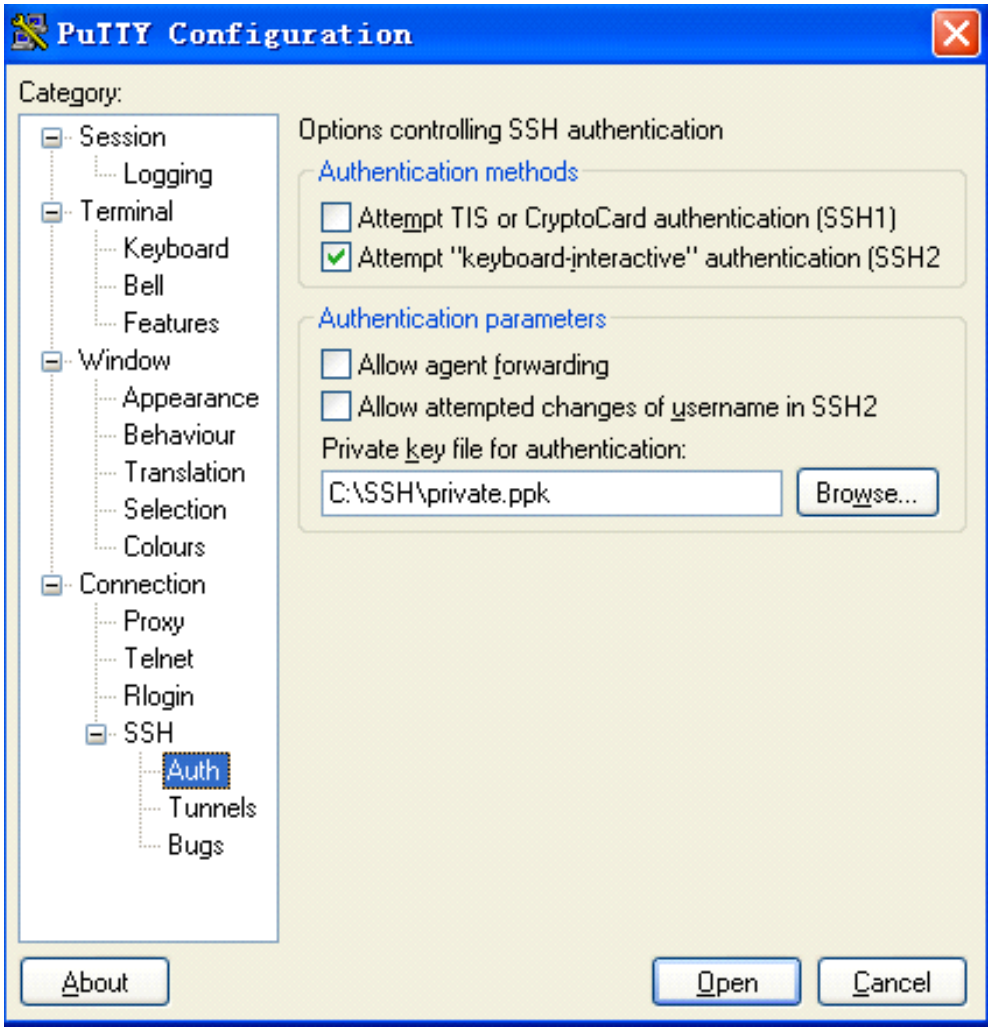
Figure 9-25 PuTTY Configuration page - RSA authentication mode (2)



Choose **Connection** > **SSH** > **Auth** in the navigation tree. The page shown in **Figure 9-26** is displayed. Select the **private.ppk** file corresponding to the public key configured on the server.

 Copyright © Huawei Technologies Co., Ltd.

Figure 9-26 PuTTY Configuration page - RSA authentication mode (3)



Click **Open**. Enter the user name at the prompt, and press **Enter**. You have logged in to the SSH server. The following information is for reference only.

```
login as: client002
Authenticating with public key "rsa-key"

<SSH Server>
```

----End

Configuration Files

SSH server configuration file

```
#
 sysname SSH Server
#
acl number 2001
 rule 5 permit source 10.137.217.10 0
 rule 10 permit source 10.137.217.20 0
 rule 15 deny source 10.137.217.30 0
#
 rsa peer-public-key rsakey001
  public-key-code begin
```

 Copyright © Huawei Technologies Co., Ltd.

```
  30820107
    02820100
      DD89041A 5E30AA97 6F384B5D B366A704 8C0E7906 EC6B088B B9567D75 914B5B4E
      A7B2E519 38D1184B 863A38BA 7E0F0DBE 5C5AE4CA 55B192B5 31AC48B0 7D21E362
      E3F2A58C 04C443CF 51CF5113 6B5B9E81 2AB1B712 50EB24A4 AE5083A1 DB18ECE2
      395C9BB8 06E8F00B E24FB516 95878440 3B617F8A AAB1F8C6 DE8C3CF0 9E4D237D
      1C17BF4A AF09C474 C083AF17 CD307533 96B32232 C57FF0B1 99197102 F1033B81
      AA6D4744 520F2368 5FAF7204 BA4B6E61 5EF22414 E64E2A33 1EEB7F18 8D980596
      DBFD300C 947A5ABA 879DC4F8 48B76951 3C35CDB5 2B291702 B77693F7 9910EE52
      87F25297 7F985E5F 186C9493 F267804E 7F5F9D52 87350A0A 4F49881B F6AB7C1B
    0201
      25
  public-key-code end
 peer-public-key end
#
aaa
 local-user client001 password irreversible-cipher %^%#*~Br";[g6Pv5Zf>$~{hY+N!`{$<[Y{;l02P)B,EBz\1FN!c+
%^%#
 local-user client001 privilege level 3
 local-user client001 service-type ssh
 local-user client002 password irreversible-cipher %^%#HW=5%Mr;:2)/RX$FnU1HLO%-TBMp4wn%;~\#
%iAut}_~O%0L%^%#
 local-user client002 privilege level 3
 local-user client002 service-type ssh
#
 ssh user client002 assign rsa-key rsakey001
 ssh user client002 authentication-type rsa
 stelnet server enable
#
user-interface vty 0 4
 acl 2001 inbound
 authentication-mode aaa
 protocol inbound ssh
#
return
```

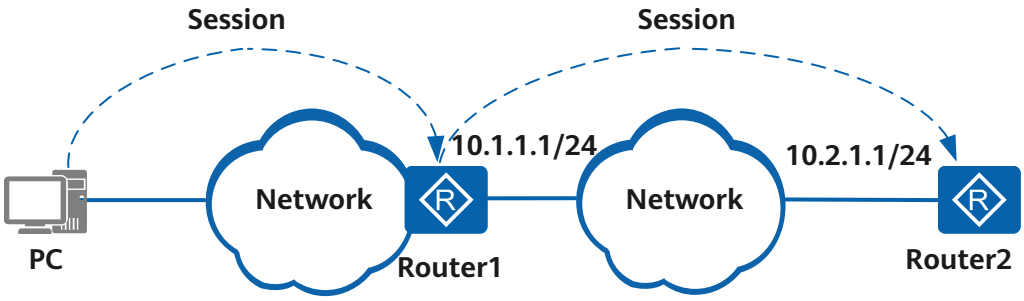
9.11.4 Example for Configuring the Device as the Telnet Client to Log In to Another Device

Networking Requirements

As shown in **Figure 9-27**, the PC and Router1 have reachable routes to each other; Router1 and Router2 have reachable routes to each other. The user needs to manage and maintain Router2 remotely. However, the PC cannot directly log in to Router2 through Telnet because it has no reachable route to Router2. The user can log in to Router1 through Telnet, and then log in to Router2 from Router1. To prevent unauthorized devices from logging in to Router2 through Telnet, an ACL needs to be configured to allow only the Telnet connection from Router1 to Router2.

 Copyright © Huawei Technologies Co., Ltd.

Figure 9-27 Networking diagram of configuring the device as the Telnet client to log in to another device



NOTE

The Telnet protocol poses a security risk, and therefore the STelnet V2 protocol is recommended.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the Telnet authentication mode and password on Router2.
2. Configure the Router2 to allow Router1 access with ACL.
3. Log in to Router2 from Router1 through Telnet.

Procedure

Step 1 Configure the Telnet authentication mode and password on Router2.

```
<Huawei> system-view
[Huawei] sysname Router2
[Router2] telnet server enable
[Router2] user-interface vty 0 4
[Router2-ui-vty0-4] user privilege level 3
[Router2-ui-vty0-4] authentication-mode aaa
[Router2-ui-vty0-4] quit
```

Step 2 Configure the login user information.

```
[Router2] aaa
[Router2-aaa] local-user admin1234 password irreversible-cipher Helloworld@6789
[Router2-aaa] local-user admin1234 service-type telnet
[Router2-aaa] local-user admin1234 privilege level 3
[Router2-aaa] quit
```

Step 3 Configure the Router2 to allow Router1 access with ACL.

```
[Router2] acl 2000
[Router2-acl-basic-2000] rule permit source 10.1.1.1 0
[Router2-acl-basic-2000] quit
[Router2] user-interface vty 0 4
[Router2-ui-vty0-4] acl 2000 inbound
[Router2-ui-vty0-4] quit
```

NOTE

It is optional to configure an ACL for Telnet services.

Step 4 Verify the configuration.

 Copyright © Huawei Technologies Co., Ltd.

After the preceding configuration, you can log in to Router2 from Router1 through Telnet. You cannot log in to Router2 from other devices. The following information is for reference only.

```
<Huawei> system-view
[Huawei] sysname Router1
[Router1] quit
<Router1> telnet 10.2.1.1
Login authentication

Username:admin1234
Password:
<Router2>
```

----End

Configuration Files

Router2 configuration file

```
#
 sysname Router2
#
acl number 2000
 rule 5 permit source 10.1.1.1 0
#
aaa
 local-user admin1234 password irreversible-cipher %^%#*~Br";[g6Pv5Zf>$~{hY+N!`{$<[Y{;l02P)B,EBz\1FN!c
+%^%#
 local-user admin1234 privilege level 3
 local-user admin1234 service-type telnet
#
 telnet server enable
#
user-interface vty 0 4
 acl 2000 inbound
 authentication-mode aaa
 user privilege level 3
#
return
```

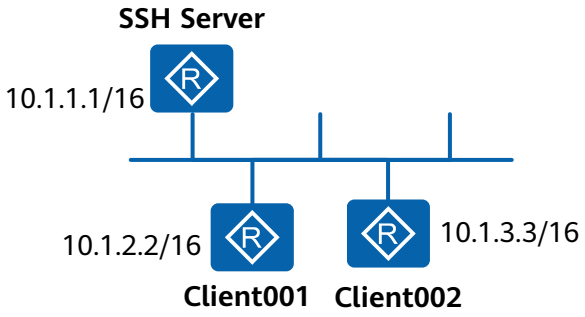
9.11.5 Example for Configuring the Device as the STelnet Client to Log In to Another Device

Networking Requirements

The enterprise requires that secure data exchange should be performed between the server and client. As shown in **Figure 9-28**, two login users **Client001** and **Client002** are configured and they use the password and RSA authentication modes respectively to log in to the SSH server. A new port number is configured and the default port number is not used.

 Copyright © Huawei Technologies Co., Ltd.

Figure 9-28 Networking diagram of logging in to another device through STelnet



NOTE

The STelnet V1 protocol poses a security risk, and therefore the STelnet V2 mode is recommended.

Configuration Roadmap

The configuration roadmap is as follows:

1. Generate a local key pair on the SSH server to implement secure data exchange between the server and client.
2. Configure different authentication modes for the SSH users **client001** and **client002** on the SSH server.
3. Enable the STelnet service on the SSH server.
4. Configure the STelnet server type for the SSH users **client001** and **client002** on the SSH server.
5. Set the SSH server listening port number on the SSH server to prevent attackers from accessing the SSH service standard port and ensure security.
6. Log in to the SSH server as the **client001** and **client002** users through STelnet.

Procedure

Step 1 Generate a local key pair on the server.

```
<Huawei> system-view
[Huawei] sysname SSH Server
[SSH Server] rsa local-key-pair create
The key name will be: Host
RSA keys defined for Host already exist.
Confirm to replace them? (y/n):y
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is less than 2048,
       It will introduce potential security risks.
Input the bits in the modulus[default = 2048]:2048
Generating keys...
.....+++
....+++
.....++++++++
.............++++++++
```

Step 2 Create an SSH user on the server.

Configure the VTY user interface.

```
[SSH Server] user-interface vty 0 4
[SSH Server-ui-vty0-4] authentication-mode aaa
[SSH Server-ui-vty0-4] protocol inbound ssh
[SSH Server-ui-vty0-4] quit
```

- Create an SSH user named **client001**.

  # Create an SSH user named **client001** and configure the password authentication mode for the user.

  ```
  [SSH Server] aaa
  [SSH Server-aaa] local-user client001 password irreversible-cipher Huawei@123
  [SSH Server-aaa] local-user client001 privilege level 3
  [SSH Server-aaa] local-user client001 service-type ssh
  [SSH Server-aaa] quit
  [SSH Server] ssh user client001 authentication-type password
  ```

- Create an SSH user named **client002**.

  # Create an SSH user named **client002** and configure the RSA authentication mode for the user.

  ```
  [SSH Server] aaa
  [SSH Server-aaa] local-user client002 password irreversible-cipher Helloworld@6789
  [SSH Server-aaa] local-user client002 privilege level 3
  [SSH Server-aaa] local-user client002 service-type ssh
  [SSH Server-aaa] quit
  [SSH Server] ssh user client002 authentication-type rsa
  ```

  # Generate a local key pair for Client002.

  ```
  <Huawei> system-view
  [Huawei] sysname client002
  [client002] rsa local-key-pair create
  The key name will be: Host
  RSA keys defined for Host already exist.
  Confirm to replace them? (y/n):y
  The range of public key size is (512 ~ 2048).
  NOTES: If the key modulus is less than 2048,
         It will introduce potential security risks.
  Input the bits in the modulus[default = 2048]:2048
  Generating keys...
  ..........................................................................+++
  ....+++
  .....................................++++++++
  ..............++++++++
  ```

  # Check the public key in the RSA key pair generated on the client.

  ```
  [client002] display rsa local-key-pair public

  =====================================================
  Time of Key pair created: 2012-08-06 17:17:37+00:00
  Key name: Host
  Key type: RSA encryption Key
  =====================================================
  Key code:
  30820109
    02820100
      CB0E88EC A1C2CFEA F97126F9 36919C08 0455127B
      A3A48594 69517096 35626F55 E4FAF0EB FDA2B9E9
      5E417B2B E09F38B0 D26FCA73 FE2E3FC4 DFBEC8CF
      4ED0C909 E8D975E6 FFC73C81 D13FE71E 759DC805
      B0F0E877 4FC9288E BE1E197C 2A7186B0 B56F5573
      3A5EA588 29C63E3B 20D56233 8E63278D F941734F
      6B359C69 BBAE5A52 EB842179 04B4204D 5DB31D72
      97F0C085 DA771F66 0AAADC28 D264CEB9 5BADA92C
      CDE9F116 D6D99C48 CEBA3A1D 868B053A 32941D85
      CCAA9796 A4B55760 0A8108ED DB45DA12 F61634C9
      59431600 341FEDEF 5379D565 A8D1953D DEA018A2
      72F99FFC 63DE04BF 2A6219BD DF13D705 27D63DEF
      83D556BC 5B44D983 8D5EA126 C1EB71CB
    0203
      010001
  ```

 Copyright © Huawei Technologies Co., Ltd.

```
=================================================
Time of Key pair created: 2012-08-06 17:17:44+00:00
Key name: Server
Key type: RSA encryption Key
=================================================
Key code:
3067
 0260
   DF8AFF3C 28213B94 2292852E E98657EE 11DE5AF4
   8A176878 CDD4BD31 55E05735 3080F367 A83A9034
   47D534CA 81250C1D 35401DC3 464E9E5F A50202CF
   A7AD09CD AC3F531C A763F0A0 4C8E51B9 18755400
   76AF4A78 225C92C3 01FE0DFF 06908363
 0203
   010001
```

Configure the RSA public key on the SSH server. (Information in bold in the **display** command output is the RSA public key. Copy the information to the server.)

```
[SSH Server] rsa peer-public-key rsakey001
[SSH Server-rsa-public-key] public-key-code begin
[SSH Server-rsa-key-code] 30820109
[SSH Server-rsa-key-code] 02820100
[SSH Server-rsa-key-code] CB0E88EC A1C2CFEA F97126F9 36919C08 0455127B
[SSH Server-rsa-key-code] A3A48594 69517096 35626F55 E4FAF0EB FDA2B9E9
[SSH Server-rsa-key-code] 5E417B2B E09F38B0 D26FCA73 FE2E3FC4 DFBEC8CF
[SSH Server-rsa-key-code] 4ED0C909 E8D975E6 FFC73C81 D13FE71E 759DC805
[SSH Server-rsa-key-code] B0F0E877 4FC9288E BE1E197C 2A7186B0 B56F5573
[SSH Server-rsa-key-code] 3A5EA588 29C63E3B 20D56233 8E63278D F941734F
[SSH Server-rsa-key-code] 6B359C69 BBAE5A52 EB842179 04B4204D 5DB31D72
[SSH Server-rsa-key-code] 97F0C085 DA771F66 0AAADC28 D264CEB9 5BADA92C
[SSH Server-rsa-key-code] CDE9F116 D6D99C48 CEBA3A1D 868B053A 32941D85
[SSH Server-rsa-key-code] CCAA9796 A4B55760 0A8108ED DB45DA12 F61634C9
[SSH Server-rsa-key-code] 59431600 341FEDEF 5379D565 A8D1953D DEA018A2
[SSH Server-rsa-key-code] 72F99FFC 63DE04BF 2A6219BD DF13D705 27D63DEF
[SSH Server-rsa-key-code] 83D556BC 5B44D983 8D5EA126 C1EB71CB
[SSH Server-rsa-key-code] 0203
[SSH Server-rsa-key-code] 010001
[SSH Server-rsa-key-code] public-key-code end
[SSH Server-rsa-public-key] peer-public-key end
```

Bind the RSA public key of the STelnet client to the SSH user client002 on the SSH server.

```
[SSH Server] ssh user client002 assign rsa-key rsakey001
```

Step 3 Enable the STelnet service on the SSH server.

Enable the STelnet service.

```
[SSH Server] stelnet server enable
```

Step 4 Configure a new listening port number on the SSH server.

```
[SSH Server] ssh server port 1025
```

Step 5 Connect the STelnet client to the SSH server.

Enable the first authentication function on the SSH client upon the first login.

Enable the first authentication function for Client001.

```
<Huawei> system-view
[Huawei] sysname client001
[client001] ssh client first-time enable
```

Enable the first authentication function for Client002.

```
[client002] ssh client first-time enable
```

 Copyright © Huawei Technologies Co., Ltd.

Log in to the SSH server from Client001 in password authentication mode by entering the user name and password.

```
[client001] stelnet 10.1.1.1 1025
Please input the username:client001
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1 ...
The server is not authenticated. Continue to access it?(y/n)[n]:y
Save the server's public key?(y/n)[n]:y
The server's public key will be saved with the name 10.1.1.1. Please wait...

Enter password:
```

Enter the password. The following information indicates that you have logged in successfully:

```
<SSH Server>
```

Log in to the SSH server from Client002 in RSA authentication mode.

```
[client002] stelnet 10.1.1.1 1025
Please input the username:client002
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1 ...
The server is not authenticated. Continue to access it?(y/n)[n]:y
Save the server's public key?(y/n)[n]:y
The server's public key will be saved with the name 10.1.1.1. Please wait...
<SSH Server>
```

The user enters the user view, indicating that login succeeds.

Step 6 Verify the configuration.

Attackers fail to log in to the SSH server using the default listening port number 22.

```
[client002] stelnet 10.1.1.1
Please input the username:client002
Trying 10.1.1.1 ...
Press CTRL+K to abort
Error: Failed to connect to the remote host.
```

Run the **display ssh server status** commands. You can see that the STelnet service has been enabled. Run the **display ssh user-information** command. Information about the configured SSH users is displayed.

Check the status of the SSH server.

```
[SSH Server] display ssh server status
 SSH version                     :1.99
 SSH connection timeout             :60 seconds
 SSH server key generating interval  :0 hours
 SSH Authentication retries         :3 times
 SFTP Server                     :Disable
 Stelnet server                  :Enable
 SSH server port                  :1025
```

Check information about SSH users.

```
[SSH Server] display ssh user-information
------------------------------------------------------------------------------
 Username        Auth-type         User-public-key-name
 -----------------------------------------------------------------------------
 client001       password          null
```

 Copyright © Huawei Technologies Co., Ltd.

```
client002       rsa             rsakey001
-------------------------------------------------------------------------------
```

----End

Configuration Files

- SSH server configuration file

```
#
 sysname SSH Server
#
 rsa peer-public-key rsakey001
  public-key-code begin
   30820109
     02820100
       E4653DA4 68032D8A B419276E 5B32743C 181FC72E AEDA3173 578EBE00 68606ED6
       D1A79735 90043220 2492B6B1 CB96BD4C E74A3209 96A829E4 EFD550FA 70855E0F
       CC622FD5 D76AD6D3 FF07F87D 19D77E06 0224D05E 481B639F 5CFB5E84 AE9FF40A
       CA2ABD4F F00B6316 6EFDADA4 7945CCC9 04C65675 22AE45C3 A2822708 AA764A40
       FBAC61F6 FB42F90C F55B1FA7 B51A58BB 4ACACD2E 7764FCCE E3B296FC 1380C0C0
       5E4A6BEE 92FB7793 E6D66E64 A3E4D581 8462C601 83C22BBF BFDF9B33 78840397
       99946916 356103D8 A791AE04 95C8A11C 3490E857 6363115B EF6A162C 6B8593A5
       8ECF3A3F 6C562154 D93B010C 932C3D18 1573F8CB D626EEA7 54F0C4E2 642BA909
     0203
       010001
  public-key-code end
 peer-public-key end
#
aaa
 local-user client001 password irreversible-cipher %^%#HW=5%Mr;:2)/RX$FnU1HLO%-TBMp4wn%;~
\#%iAut}_~O%0L%^%#
 local-user client001 privilege level 3
 local-user client001 service-type ssh
 local-user client002 password irreversible-cipher %^%#*~Br";[g6Pv5Zf>$~{hY+N!`{$<[Y{;l02P)B,EBz
\1FN!c+%^%#
 local-user client002 privilege level 3
 local-user client002 service-type ssh
#
 ssh user client002 assign rsa-key rsakey001
 ssh user client002 authentication-type rsa
 stelnet server enable
 SSH server port 1025
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
#
return
```

- Client001 configuration file

```
#
 sysname client001
#
ssh client first-time enable
#
return
```

- Client002 configuration file

```
#
 sysname client002
#
ssh client first-time enable
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

9.11.6 Example for Logging In to Another Device Through Redirection

Networking Requirements

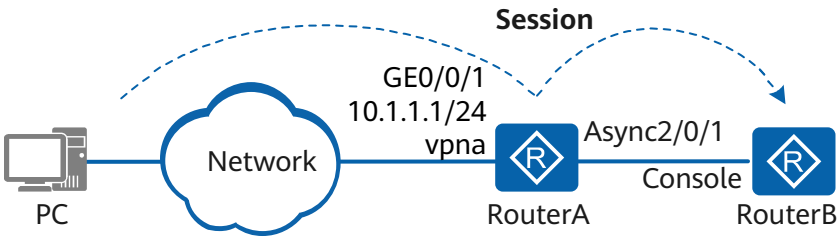
In telecommunication and financial fields, some terminals provide only access through the serial port or cannot access the Internet using Telnet. The serial port redirection of the router enables you to configure and manage terminals connected to the router through Telnet.

As shown in **Figure 9-29**, the asynchronous serial port on RouterA connects to the console port on RouterB through an asynchronous serial cable. You can log in to RouterB through RouterA from the remote PC in **vpna**. RouterA functions as the serial port server and there is a reachable route between the remote PC and RouterA. You can log in to RouterB connected to RouterA from the remote PC using the IP address and specified port number.

NOTE

For details about the asynchronous serial cable, see "8AS Cable" in the *Huawei AR Series Access Routers Get to Know the Product - Hardware Description - Cables*.

Figure 9-29 Networking diagram for redirection configuration



Configuration Roadmap

The configuration roadmap is as follows:

1. Connect the console port of RouterB to an asynchronous serial port of RouterA.
2. Enable the redirection function on RouterA.

Procedure

Step 1 Configure the asynchronous serial port to work in flow mode.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface async 2/0/1
[RouterA-Async2/0/1] async mode flow
```

Step 2 Obtain the TTY user interface number corresponding to the asynchronous serial port.

```
[RouterA] display user-interface
  Idx  Type     Tx/Rx      Modem Privi ActualPrivi Auth  Int
```

 Copyright © Huawei Technologies Co., Ltd.

```
  0    CON 0    9600      -     15    -         N     -
  41   TTY 41   9600      inout 0     -         N     2/0/0
  42   TTY 42   9600      -     0     -         N     2/0/1
  43   TTY 43   9600      -     0     -         N     2/0/2
  44   TTY 44   9600      -     0     -         N     2/0/3
  45   TTY 45   9600      -     0     -         N     2/0/4
  46   TTY 46   9600      -     0     -         N     2/0/5
  47   TTY 47   9600      -     0     -         N     2/0/6
  48   TTY 48   9600      -     0     -         N     2/0/7
+ 129  VTY 0              -     15    4         N     -
  130  VTY 1              -     15    -         N     -
  131  VTY 2              -     15    -         N     -
  132  VTY 3              -     15    -         N     -
  133  VTY 4              -     15    -         N     -
  145  VTY 16             -     0     -         P     -
  146  VTY 17             -     0     -         P     -
  147  VTY 18             -     0     -         P     -
  148  VTY 19             -     0     -         P     -
  149  VTY 20             -     0     -         P     -
```

Step 3 Configuring a VPN Instance **vpna**.

```
[RouterA] ip vpn-instance vpna
[RouterA-vpn-instance-vpna] route-distinguisher 1:1
[RouterA-vpn-instance-vpna-af-ipv4] vpn-target 111:1 export-extcommunity
[RouterA-vpn-instance-vpna-af-ipv4] vpn-target 111:1 import-extcommunity
[RouterA-vpn-instance-vpna-af-ipv4] quit
[RouterA-vpn-instance-vpna] quit
[RouterA] interface gigabitethernet 0/0/1
[RouterA-GigabitEthernet0/0/1] ip binding vpn-instance vpna
[RouterA-GigabitEthernet0/0/1] ip address 10.1.1.1 255.255.255.0
[RouterA-GigabitEthernet0/0/1] quit
```

Step 4 Enable the redirection function on RouterA and associate the redirection function with the VPN instance **vpna**.

```
[RouterA] user-interface tty 42
[RouterA-ui-tty42] undo shell
[RouterA-ui-tty42] redirect enable
[RouterA-ui-tty42] redirect binding vpn-instance vpna
[RouterA-ui-tty42] authentication-mode password
[RouterA-ui-tty42] set authentication password cipher
Enter Password(<8-128>):
Confirm password:
[RouterA-ui-tty42] quit
[RouterA] quit
```

NOTE

If the redirection function is not associated with the VPN instance to which the private users belong, all users on public and private networks can log in to RouterB.

Step 5 Check the port number allocated to the TTY user interface.

```
<RouterA> display tcp status
TCPCB    Tid/Soid Local Add:port       Foreign Add:port      VPNID  State
19fde824 9  /2    0.0.0.0:22           0.0.0.0:0             23553  Listening
19fde6c0 9  /1    0.0.0.0:23           0.0.0.0:0             23553  Listening
19fde130 109/1    0.0.0.0:80           0.0.0.0:0             23553  Listening
19fdef18 9  /4    0.0.0.0:2042         0.0.0.0:0             23553  Listening
19fde55c 7  /1    0.0.0.0:7547         0.0.0.0:0             0      Listening
19fdf07c 9  /9    10.137.217.211:23    10.138.77.61:2567     0      Established
19fdf344 9  /10   10.137.217.211:23    10.138.77.69:2824     0      Time_Wait
```

Step 6 Verify the configuration.

Run the **telnet 10.1.1.1 2042** command on the PC to log in to RouterB. By default, the port number is 2000 plus *tty-number*.

```
C:\Documents and Settings\Administrator> telnet 10.1.1.1 2042
Press CTRL_] to quit telnet mode
  Trying 10.1.1.1...
```

 Copyright © Huawei Technologies Co., Ltd.

```
  Connected to 10.1.1.1...
Login authentication


Password:
 <RouterB>
```

----End

Configuration Files

- Configuration file of RouterA

```
#
 sysname RouterA
#
ip vpn-instance vpna
 ipv4-family
  route-distinguisher 1:1
  vpn-target 111:1 export-extcommunity
  vpn-target 111:1 import-extcommunity
#
interface Async2/0/1
 async mode flow
#
interface GigabitEthernet0/0/1
 ip binding vpn-instance vpna
 ip address 10.1.1.1 255.255.255.0
#
user-interface tty 42
 authentication-mode password
 set authentication password cipher %^%##N&)XdgB87~RcnU9upv6,.d;,uXe*#IeE-ywBaSmj:\@.d>,%^
%#
 redirect enable
 redirect binding vpn-instance vpna
#
return
```

9.11.7 Example for Configuring an NMS to Communicate with a Device by SSH over a VPN

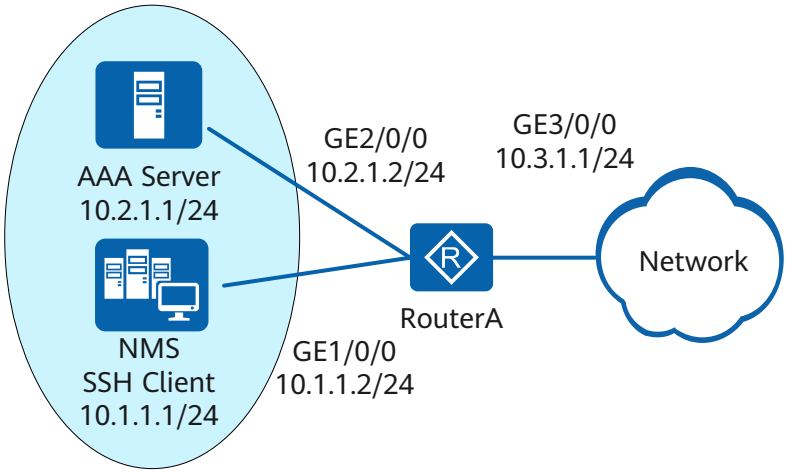
This section provides an example for configuring an NMS to communicate with a device by SSH over a VPN.

Networking Requirements

On the network shown in **Figure 9-30**, an NMS, Router A, and AAA server are connected over a VPN. The NMS is integrated with the SSH client and SFTP server functions. The SSH client uses SSH to log in to and communicate with the Router A. The SFTP server uses SFTP for file transfer with the Router A functioning as an SFTP client.

 Copyright © Huawei Technologies Co., Ltd.

Figure 9-30 Networking diagram for configuring an NMS to communicate with a device by SSH over a VPN



NOTE

The interfaces are bound to the same VPN instance.

Precautions

Ensure that the route between the device and NMS is reachable.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a VPN instance.
2. Bind the interfaces connecting the device to the NMS and HWTACACS server to the VPN instance.
3. Configure a default VPN instance used by the NMS to manage the device.
4. Configure an HWTACACS server.
5. Configure a local AAA user and set its access mode to SSH and authentication mode to HWTACACS.
6. Configure an SSH user and set its authentication and service modes.
7. Configure an SNMPv3 USM user to allow the NMS to access the device.
8. Configure an SFTP client to use SFTP for file transfer.

Procedure

Step 1 Configure a VPN instance.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] ip vpn-instance vrf1
[RouterA-vpn-instance-vrf1] ipv4-family
[RouterA-vpn-instance-vrf1-af-ipv4] route-distinguisher 22:1
[RouterA-vpn-instance-vrf1-af-ipv4] vpn-target 111:1 both
[RouterA-vpn-instance-vrf1-af-ipv4] quit
[RouterA-vpn-instance-vrf1] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Step 2 Bind interfaces to the VPN instance.

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip binding vpn-instance vrf1
[RouterA-GigabitEthernet1/0/0] ip address 10.1.1.2 255.255.255.0
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip binding vpn-instance vrf1
[RouterA-GigabitEthernet2/0/0] ip address 10.2.1.2 255.255.255.0
[RouterA-GigabitEthernet2/0/0] quit
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] ip binding vpn-instance vrf1
[RouterA-GigabitEthernet3/0/0] ip address 10.3.1.1 255.255.255.0
[RouterA-GigabitEthernet3/0/0] quit
```

Step 3 Configure a default VPN instance used by the NMS to manage the device.

```
[RouterA] set net-manager vpn-instance vrf1
```

NOTE

The VPN configured using this command affects the following service modules on the device: TFTP client, FTP client, SFTP client, SCP client, Info Center, SNMP, PM, IP FPM, and TACACS. To access the public network, you must set the public-net parameter.

Step 4 Configure an HWTACACS server.

Enable the HWTACACS function and configure an HWTACACS server template named ht.

```
[RouterA] hwtacacs enable
[RouterA] hwtacacs-server template ht
```

Configure an IP address and a VPN instance to which the HWTACACS accounting server is bound for the primary HWTACACS authentication and authorization server.

```
[RouterA-hwtacacs-ht] hwtacacs-server authentication 10.2.1.1 vpn-instance vrf1
[RouterA-hwtacacs-ht] hwtacacs-server authorization 10.2.1.1 vpn-instance vrf1
```

Configure a key for the server.

```
[RouterA-hwtacacs-ht] hwtacacs-server shared-key cipher it-is-my-secret123
[RouterA-hwtacacs-ht] quit
```

Enter the AAA view.

```
[RouterA] aaa
```

Configure an authentication scheme named scheme1 and set the authentication mode to HWTACACS authentication.

```
[RouterA-aaa] authentication-scheme scheme1
[RouterA-aaa-authen-scheme1] authentication-mode hwtacacs
[RouterA-aaa-authen-scheme1] quit
```

Configure an authorization scheme named scheme2 and set the authorization mode to HWTACACS authorization.

```
[RouterA-aaa] authorization-mode scheme2
[RouterA-aaa-authen-scheme2] authorization-mode hwtacacs
[RouterA-aaa-authen-scheme2] quit
```

Configure the huawei domain. Use the scheme1 authentication scheme, scheme2 authorization scheme, and ht template in the domain.

```
[RouterA-aaa] domain huawei
[RouterA-aaa-domain-huawei] authentication-scheme scheme1
[RouterA-aaa-domain-huawei] authorization-mode scheme2
```

 Copyright © Huawei Technologies Co., Ltd.

```
[RouterA-aaa-domain-huawei] hwtacacs-server ht
[RouterA-aaa-domain-huawei] quit
```

Step 5 Create a local AAA user named sshuser001. Set the access mode to SSH and authentication mode to HWTACACS.

Configure a local user named sshuser001 in the huawei domain. After the configuration is complete, the sshuser001 user uses the authentication and authorization modes in the huawei domain.

```
[RouterA-aaa] local-user sshuser001@huawei password
Please configure the password (8-128)
Enter Password:
Confirm Password:
[RouterA-aaa] local-user sshuser001@huawei service-type ssh
[RouterA-aaa] quit
```

Step 6 Configure authentication for the SSH user.

```
[RouterA] ssh user sshuser001 authentication-type password
```

Step 7 Enable the STelnet.

```
[RouterA] stelnet server enable
```

Step 8 Configure an SNMPv3 USM user to allow the NMS to access the device.

Enable the SNMP agent function.

```
[RouterA] snmp-agent
```

Set the SNMP version to SNMPv3.

```
[RouterA] snmp-agent sys-info version v3
```

Configure a MIB view.

```
[RouterA] snmp-agent mib-view iso include iso
```

Configure a user group and users in the group, and authenticate and encrypt user data.

```
[RouterA] snmp-agent group v3 admin privacy write-view iso notify-view iso read-view iso
[RouterA] snmp-agent usm-user v3 nms-admin group admin
[RouterA] snmp-agent usm-user v3 nms-admin authentication-mode sha
Please configure the authentication password (10-255)
Enter Password:
Confirm Password:
[RouterA] snmp-agent usm-user v3 nms2-admin privacy-mode aes128
Please configure the privacy password (10-255)
Enter Password:
Confirm Password:
```

Configure the alarm function.

```
[RouterA] snmp-agent target-host trap-hostname aaa address 10.1.1.1 trap-paramsnam abc
[RouterA] snmp-agent trap enable
```

Step 9 Enable the device functioning as an SFTP client to transfer files with the NMS functioning as an SFTP server over the VPN.

```
[RouterA] ssh client first-time enable
[RouterA] sftp 10.1.1.1
[RouterA] put aaa.cfg
```

Step 10 Verify the configuration.

After completing the configuration, perform the following operations to check whether the configuration takes effect.

 Copyright © Huawei Technologies Co., Ltd.

Display the SNMP version.

```
[RouterA] display snmp-agent sys-info version
  SNMP version running in the system:
        SNMPv3
```

Display information about an SNMPv3 user.

```
[RouterA] display snmp-agent usm-user
  User name: nms-admin,
  Engine ID: 800007DB0300259E0370C3 active
  Group-name: admin
  Authentication mode: sha
  Privacy mode: aes128
  User state: Active
```

----End

Configuration Files

- Router A configuration file

```
#
sysname RouterA
#
hwtacacs enable
#
ip vpn-instance vrf1
 ipv4-family
  route-distinguisher 22:1
  vpn-target 111:1 export-extcommunity
  vpn-target 111:1 import-extcommunity
#
hwtacacs-server template ht
 hwtacacs-server authentication 10.2.1.1 vpn-instance vrf1
 hwtacacs-server authorization 10.2.1.1 vpn-instance vrf1
 hwtacacs-server shared-key cipher %^%#x@ZaCImt|
X79[^A&]DEYC6[>U]OD(8n&BVHvsu2R{=zVSySB'|H[;I`|ef#%^%#
#
aaa
 local-user sshuser001@huawei password irreversible-cipher $1c$\h[;D"`M79$GN]A=y;*4EFG
%t>vIJI=rJvxWe/V%Xbd;(J+AzC+$
 local-user sshuser001@huawei service-type ssh
 #
 authentication-scheme scheme1
  authentication-mode hwtacacs
 #
 authorization-scheme scheme2
  authorization-mode hwtacacs
 #
 accounting-scheme default0
 #
 accounting-scheme default1
 #
 domain huawei
  authentication-scheme scheme1
  authorization-scheme scheme2
  hwtacacs-server ht
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip binding vpn-instance vrf1
 ip address 10.1.1.2 255.255.255.0
interface GigabitEthernet2/0/0
 undo shutdown
 ip binding vpn-instance vrf1
 ip address 10.2.1.2 255.255.255.0
interface GigabitEthernet3/0/0
 undo shutdown
```

 Copyright © Huawei Technologies Co., Ltd.

```
 ip binding vpn-instance vrf1
 ip address 10.3.1.1 255.255.255.0
#
snmp-agent
snmp-agent local-engineid 800007DB0300313D6A1FA0
#
snmp-agent sys-info version v3
snmp-agent group v3 admin privacy write-view iso notify-view iso read-view iso
snmp-agent target-host trap-hostname aaa address 10.1.1.1 trap-paramsnam abc
#
snmp-agent mib-view iso include iso
snmp-agent usm-user v3 nms-admin group admin
snmp-agent usm-user v3 nms-admin authentication-mode sha %#%##/L&Fd]S.!i*S7<\jCh2DkfkE4+:<
%Wap|8zZWwPL+[a>h$wy>VJsp9(L{%B%#%#
snmp-agent usm-user v3 nms-admin privacy-mode aes128 %#
%#CM-]HDuhH6VX)**J<186nf({M823f(0Z73++7(A#%,1jODj}D>_HS>W,'Ss=%#%#
#
stelnet server enable
ssh user sshuser001 authentication-type password
#
ssh client first-time enable
#
return
```

9.12 Troubleshooting CLI Login

This section describes common faults caused by incorrect configurations and provides the corresponding troubleshooting procedures.

9.12.1 Failing to Log In Through the Console Port

Fault Description

Login through the console port fails.

Procedure

Step 1 Check whether the serial port parameters are correctly configured. (The third-party software PuTTY is used as an example here.)

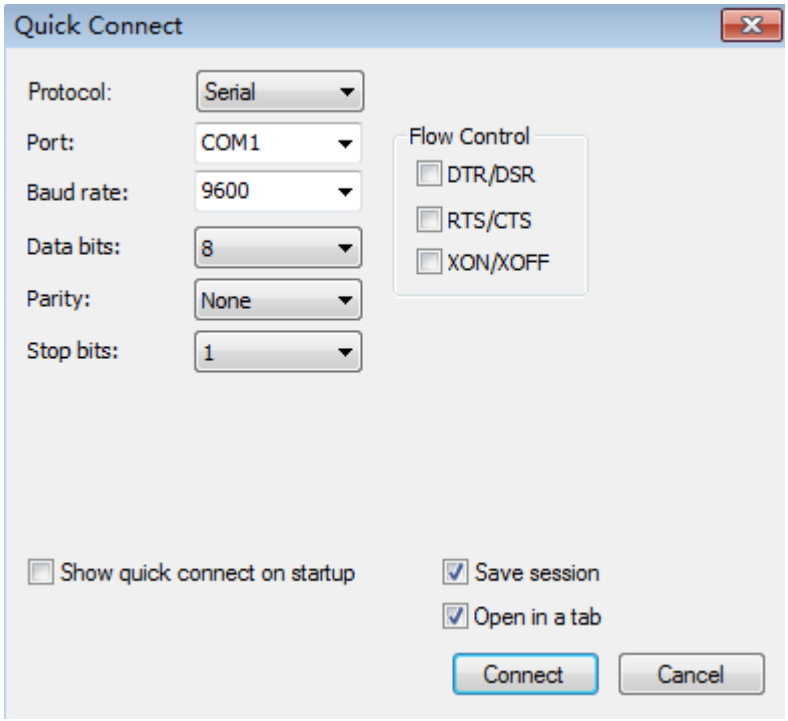
Check whether a correct serial port is connected. Some PCs provide multiple serial ports with corresponding numbers. When connecting a serial port, ensure that the correct serial port number is selected.

Check that the serial port settings on the PC are the same as the console port settings on the device, as shown in **Figure 9-31**. The default console port settings are as follows:

- Baud rate: 9600
- Data bits: 8
- Stop bits: 1
- Parity: None
- Flow control: None

 Copyright © Huawei Technologies Co., Ltd.

Figure 9-31 Setting the connected port and communication parameters



Step 2 Check whether the serial cable is securely connected. If necessary, replace the current cable with a properly-functioning one.

----End

9.12.2 Failing to Log In Through Telnet

Fault Description

The Telnet server fails to be logged in through Telnet.

Procedure

Step 1 Check whether the number of login users reaches the upper limit.

Log in to the device through the console port and run the **display users** command to check whether all VTY user interfaces are in use. By default, the maximum number of VTY user interfaces is 5. You can run the **display user-interface maximum-vty** command to check the maximum number of login users allowed by the device.

If the number of login users reaches the upper limit, run the **user-interface maximum-vty** 15 command to increase the maximum number of login users to 15.

Step 2 Check whether an ACL is configured in the VTY user interface view (Telnet IPv4 is used as an example).

Run the **user-interface vty** command on the Telnet server to enter the user interface view and then run the **display this** command to check whether an ACL is configured in the VTY user interface view. If so, record the ACL number.

 Copyright © Huawei Technologies Co., Ltd.

Run the **display acl** *acl-number* command on the Telnet server to check whether the IP address of the Telnet client is denied in the ACL. If so, run the **undo rule** *rule-id* command in the ACL view to delete the **deny** rule and then run the corresponding command to modify the ACL and permit the IP address of the client.

Step 3 Check whether the access protocol is correctly configured in the VTY user interface view.

Run the **user-interface vty** command on the Telnet server to enter the user interface view and then run the **display this** command to check whether **protocol inbound** is set to **telnet** or **all**. By default, the system supports the SSH and Telnet protocol. If not, run the **protocol inbound** { **telnet** | **all** } command to allow Telnet users to connect to the device.

Step 4 Check whether an authentication mode is set for login users in the user interface view.

- If password authentication is configured using the **authentication-mode password** command, you must enter the password upon login.
- If AAA authentication is configured using the **authentication-mode aaa** command, you must run the **local-user** command to create a local AAA user.

----End

9.12.3 Failing to Log In Through STelnet

Fault Description

The SSH server fails to be logged in through STelnet.

Procedure

Step 1 Check whether the SSH service is enabled on the SSH server.

Log in to the SSH server through the console port or using Telnet and run the **display ssh server status** command to check the SSH server configuration.

If the STelnet service is disabled, run the **stelnet server enable** command to enable the STelnet service on the SSH server.

Step 2 Check whether the access protocol is correctly configured in the VTY user interface view.

Run the **user-interface vty** command on the SSH server to enter the user interface view and then run the **display this** command to check whether **protocol inbound** is set to **ssh** or **all**. If not, run the **protocol inbound** { **ssh** | **all** } command to allow STelnet users to log in to the device.

Step 3 Check whether an RSA public key is configured on the SSH server.

A local key pair must be configured when the device works as the SSH server.

Run the **display rsa local-key-pair public** command on the SSH server to check the current key pair. If no information is displayed, no key pair is configured on the server. Run the **rsa local-key-pair create** command to create a key pair.

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

To ensure high security, it is recommended that the RSA authentication mode be not used.

Step 4 Check whether an SSH user is configured on the SSH server.

Run the **display ssh user-information** command to view the SSH user configuration. If no configuration is available, run the **ssh user authentication-type** commands in the system view to create an SSH user and set an authentication mode for the SSH user.

Step 5 Check whether the number of login users on the SSH server reaches the upper limit.

Log in to the device through the console port and run the **display users** command to check whether all VTY user interfaces are in use. By default, the maximum number of VTY user interfaces is 5. You can run the **display user-interface maximum-vty** command to check the maximum number of login users allowed by the device.

If the number of login users reaches the upper limit, run the **user-interface maximum-vty** 15 command to increase the maximum number of login users to 15.

Step 6 Check whether an ACL is bound to the VTY user interface of the SSH server.

Run the **user-interface vty** command on the SSH server to enter the user interface view and then run the **display this** command to check whether an ACL is configured on the VTY user interface. If so, record the ACL number.

Run the **display acl** *acl-number* command on the SSH server to check whether the IP address of the STelnet client is denied in the ACL. If so, run the **undo rule** *rule-id* command in the ACL view to delete the **deny** rule and then run the corresponding command to modify the ACL and permit the IP address of the client.

Step 7 Check the SSH version on the SSH client and server.

Run the **display ssh server status** command on the SSH server to check the SSH version.

If the SSHv1 client logs in, run the **ssh server compatible-ssh1x enable** command to enable the version compatibility function on the server.

Step 8 Check whether first-time authentication is enabled on the SSH client.

Run the **display this** command in the system view on the SSH client to check whether first-time authentication is enabled on the SSH client.

If not, the initial login of the SSH client fails because validity check on the public key of the SSH server fails. Run the **ssh client first-time enable** command to enable first-time authentication on the SSH client.

----End

 Copyright © Huawei Technologies Co., Ltd.

9.13 FAQ About CLI Login

This section describes common problems you may encounter during the configuration and provides the solutions to these problems.

9.13.1 What Is the Default Login Password?

The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

NOTE

For security purposes, you are advised to change the default password for the device.

9.13.2 What If I Forget the Password for Console Port Login?

Procedure

When you forget the password for logging in through the console port, use either of the following two methods to set a new password.

Logging In to the Device Through STelnet/Telnet to Set a New Password

NOTICE

It is recommended that you use STelnet V2 to log in to the device.

The following uses the command lines and outputs of logging in to the device using STelnet as an example. After logging in to the device through STelnet, perform the following operations.

Take password authentication as an example. Set the password to **Huawei@123**.

```
<Huawei> system-view
[Huawei] user-interface console 0
[Huawei-ui-console0] authentication-mode password
[Huawei-ui-console0] set authentication password cipher
Warning: The "password" authentication mode is not secure, and it is strongly re
commended to use "aaa" authentication mode.
Enter Password(<8-128>):
Confirm password:
[Huawei-ui-console0] return
<Huawei> save
```

Take AAA authentication as an example. Set the user name and password to **admin123** and **Huawei@123**, respectively.

```
<Huawei> system-view
[Huawei] user-interface console 0
[Huawei-ui-console0] authentication-mode aaa
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-ui-console0] quit
[Huawei] aaa
[Huawei-aaa] local-user admin123 password irreversible-cipher Huawei@123
[Huawei-aaa] local-user admin123 privilege level 15
[Huawei-aaa] local-user admin123 service-type terminal
[Huawei-aaa] return
<Huawei> save
```

Clearing the Lost Password Using the BootROM Menu

You can use the BootROM menu of the device to clear the lost password for console port login. After starting the device, set a new password and save your configuration. Perform the following steps.

1. Connect the terminal to the console port of the device and restart the device. When the following message is displayed, press **Ctrl+B** and enter the BootROM password to enter the BootROM menu.

   ```
   Press Ctrl+B to break auto startup ... 1

   Enter Password:      //Enter the BootROM password.
   ```

2. In the BootROM menu, select **Password Manager** and then **Clear the console login password**.
3. Then select the **Return** and **Default Startup** options in turn to restart the device.
4. After the system starts, you can log in through the console port without password authentication. After logging in to the system, set an authentication mode and password for the console user interface as required. The configuration is similar to that of Logging In to the Device Through STelnet/Telnet to Set a New Password, and is not provided here.

   NOTE

   Configuring the authentication mode and password for the console user interface is necessary; otherwise, after the device is restarted, users still need to be authenticated using the original password when they log in to the device through the console port.

More Information

- When you log in to the device through STelnet/Telnet to set a new password: Ensure that you have an STelnet/Telnet account and administrator rights.
- When you clear the lost password using the BootROM Menu, if you do not press **Ctrl+B** within the timeout (several seconds), you have to restart the router again.

9.13.3 What If I Forget the Password for Telnet Login?

Procedure

If you forget the Telnet login password, log in to the device through the console port and set a new password for Telnet login.

Take password authentication for VTY0 login as an example. Set the password to **Huawei@123**.

```
<Huawei> system-view
[Huawei] user-interface vty 0
[Huawei-ui-vty0] authentication-mode password
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-ui-vty0] set authentication password cipher
Warning: The "password" authentication mode is not secure, and it is strongly re
commended to use "aaa" authentication mode.
Enter Password(<8-128>):
Confirm password:
[Huawei-ui-vty0] user privilege level 15
[Huawei-ui-vty0] return
<Huawei> save
```

Take AAA authentication for VTY0 login as an example. Set the user name and password to **admin123** and **Huawei@123**, respectively.

```
<Huawei> system-view
[Huawei] user-interface vty 0
[Huawei-ui-vty0] protocol inbound telnet
[Huawei-ui-vty0] authentication-mode aaa
[Huawei-ui-vty0] quit
[Huawei] aaa
[Huawei-aaa] local-user admin123 password irreversible-cipher Huawei@123
[Huawei-aaa] local-user admin123 service-type telnet
[Huawei-aaa] local-user admin123 privilege level 15
[Huawei-aaa] return
<Huawei> save
```

More Information

By default, a user only needs to pass password authentication to log in to the device from the console user interface. To prevent unauthorized users from accessing the device, change the authentication mode of the console user interface to AAA authentication.

9.13.4 How Do I Configure Screen Display?

- Setting the number of rows displayed on a screen

  Run the **screen-length** *screen-length* [**temporary**] command in the user view or user interface view to set the number of rows to be displayed on a screen.

  You must specify **temporary** when running the command in the user view. The configured value takes effect only on the current VTY user interface but does not take effect on the next login on the same user interface or login on other VTY user interfaces.

  The default number of rows to be displayed on a screen is 24.

- Setting the number of columns displayed on a screen

  Run the **screen-width** *screen-width* command in any view to set the number of columns to be displayed on a screen.

  The default number of columns to be displayed on a screen is 80. Each character is a column.

9.13.5 How Do I Force an Online User to Go Offline?

You can run the **free user-interface** { *ui-number* | *ui-type ui-number1* } command to remove a user from a specified user interface, that is, disconnect the user from the device.

 Copyright © Huawei Technologies Co., Ltd.

This command does not take effect for the current user. For example, if the user interface of the current user is VTY 2, the **free user-interface vty 2** command does not take effect and the system displays an error message.

```
<Huawei> free user-interface 0
Warning: User interface Console1 will be freed. Continue? [Y/N]:y
```

9.13.6 What Are System Users of AR Routers?

Table 9-7 lists the user accounts in the system.

Table 9-7 User accounts

User	Usage Description	Remarks
root	The **root** user is the default user in the system and is unavailable to an external system.	This account cannot be used to log in to the system directly. When this account is used to run a command, the system automatically checks and authenticates the account.
huawei	The **huawei** user is used to execute application programs. This user is a system user and cannot be used to log in to the system.	This account cannot be used to log in to the system directly. When this account is used to run a command, the system automatically checks and authenticates the account.
python	The **python** user is used to run Python scripts in the system and is unavailable to an external system.	This account cannot be used to log in to the system directly. When this account is used to run a command, the system automatically checks and authenticates the account.
bin	On Linux, this user is a built-in user, which does not have a password and cannot be used to log in to the system.	This account cannot be used.
daemon	On Linux, this user is a built-in user, which does not have a password and cannot be used to log in to the system.	This account cannot be used.

 Copyright © Huawei Technologies Co., Ltd.

User	Usage Description	Remarks
lp	On Linux, this user is a built-in user, which does not have a password and cannot be used to log in to the system.	This account cannot be used.
sync	On Linux, this user is a built-in user, which does not have a password and cannot be used to log in to the system.	This account cannot be used.
mail	On Linux, this user is a built-in user, which does not have a password and cannot be used to log in to the system.	This account cannot be used.
uucp	On Linux, this user is a built-in user, which does not have a password and cannot be used to log in to the system.	This account cannot be used.
games	On Linux, this user is a built-in user, which does not have a password and cannot be used to log in to the system.	This account cannot be used.
sys	On Linux, this user is a built-in user, which does not have a password and cannot be used to log in to the system.	This account cannot be used.
man	On Linux, this user is a built-in user, which does not have a password and cannot be used to log in to the system.	This account cannot be used.
news	On Linux, this user is a built-in user, which does not have a password and cannot be used to log in to the system.	This account cannot be used.
proxy	On Linux, this user is a built-in user, which does not have a password and cannot be used to log in to the system.	This account cannot be used.

 Copyright © Huawei Technologies Co., Ltd.

User	Usage Description	Remarks
www-data	On Linux, this user is a built-in user, which does not have a password and cannot be used to log in to the system.	This account cannot be used.
backup	On Linux, this user is a built-in user, which does not have a password and cannot be used to log in to the system.	This account cannot be used.
list	On Linux, this user is a built-in user, which does not have a password and cannot be used to log in to the system.	This account cannot be used.
irc	On Linux, this user is a built-in user, which does not have a password and cannot be used to log in to the system.	This account cannot be used.
gnats	On Linux, this user is a built-in user, which does not have a password and cannot be used to log in to the system.	This account cannot be used.
nobody	On Linux, this user is a built-in user, which does not have a password and cannot be used to log in to the system.	This account cannot be used.
tss	The **tss** user is an open-source TCG Software Stack (TSS) user. This user is a card-level user without a password and is unavailable to an external system. This account cannot be used to log in to the system directly.	This account cannot be used.

 Copyright © Huawei Technologies Co., Ltd.

10 Web System Login Configuration

About This Chapter

This chapter describes how to log in to a device through the web system to manage and maintain the device.

AR routers support the web system. You can run commands to configure a device's management IP address, upload and load the web page file, create a web system account, and configure web system parameters. After the configuration is complete, you can log in to and maintain the device through the web system.

You can also use the default factory settings to directly log in to the web system for device management and maintenance. For details, see Logging In to the Device.

10.1 Overview of Web System Login

10.2 Licensing Requirements and Limitations for Web System Login
This section provides the configuration precautions of web system login.

10.3 Default Settings for Web System Login
This section describes the default settings for web system login.

10.4 Configuring Device Login Through the Web System
This section describes how to configure device login through the web system.

10.5 Configuration Examples for Web System Login
This section provides an example for configuring device login through the web system.

10.6 Common Misconfigurations
This section describes common faults caused by incorrect configurations and provides the troubleshooting procedure.

10.7 FAQ About Web System Login
This section describes common problems you may encounter during the configuration and provides the solutions to these problems.

 Copyright © Huawei Technologies Co., Ltd.

10.1 Overview of Web System Login

This section describes the definition, purpose, and concepts of the web system.

Definition

The web system is a built-in web server on the device and provides a graphical user interface (GUI) for users. Before using the web system to manage and maintain a device, you need to log in to the device from a terminal using Hypertext Transfer Protocol Secure (HTTPS).

Purpose

You can manage a device on the command line interface (CLI) or web system.

- The CLI mode requires you to use commands to manage and maintain the device. This mode realizes fine-grained device management, but requires you to be familiar with the commands.
- The web system mode allows you to easily manage and maintain the device on a GUI. However, you can only use this mode to manage and maintain some functions on the device.

You can select a proper management mode based on actual requirements.

To use the CLI, you must log in to the device through the console port or MiniUSB port, or using Telnet or STelnet. To use the web system, you must log in to the device using HTTPS.

NOTE

For details about how to log in to a device through the console port or MiniUSB port, or using Telnet or STelnet, see **CLI Login Configuration**.

10.2 Licensing Requirements and Limitations for Web System Login

This section provides the configuration precautions of web system login.

Involved Network Elements

None

Licensing Requirements

Web System Login is a basic feature of a router and is not under license control.

Feature Limitations

None

 Copyright © Huawei Technologies Co., Ltd.

10.3 Default Settings for Web System Login

This section describes the default settings for web system login.

Table 10-1 lists the default settings for web system login.

Table 10-1 Default settings for web system login

Parameter	Default Setting
Web page file integrated into system software	Supported
Default SSL policy	Supported
HTTPS service	Enabled
Port number of the HTTPS server	443
HTTPS session timeout interval	10 minutes
Web user	The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.
Access control on web users	None

10.4 Configuring Device Login Through the Web System

This section describes how to configure device login through the web system.

Pre-configuration Tasks

Before configuring device login through the web system, complete the following task:

Log in to the device using the CLI mode. For details, see **CLI Login Configuration**.

Configuration Process

10.4.1 Configuring a Management IP Address for the Device

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Run **system-view**

The system view is displayed.

Step 2 Run **interface** *interface-type interface-number*

The interface view is displayed.

Step 3 Run **ip address** *ip-address* { *mask* | *mask-length* }

A management IP address is configured.

NOTE

The factory settings of the device include the IP address 192.168.1.1 and subnet mask 255.255.255.0. The access interface is the management interface under which the silkscreen **Management** or **MGMT** is printed.

----End

10.4.2 (Optional) Uploading and Loading the Web Page File

Context

The system software contains the web page file. The web page file is loaded on the device when the system software is loaded. If new system software is uploaded to the device, you do not need to perform the following operations.

Under special circumstances, Huawei releases independent web page files matching some system software versions. After obtaining these web page files, you can upload the files to devices using SFTP and other modes, and then load the files on the devices.

Procedure

Step 1 Upload the web page file.

You can upload the web page file using SFTP or other modes. For details, see **Local File Management**.

NOTE

After uploading the web page file, run the **dir** command in the user view to check whether the web page file on the device has the same size as that on the file server. If not, an exception may occur during file upload. Upload the file again.

Step 2 Load the web page file.

1. Run **system-view**

   The system view is displayed.

2. Run **http server load** *file-name*

   The web page file is loaded.

 Copyright © Huawei Technologies Co., Ltd.

By default, the web page file in the system software is loaded on the device.

----End

10.4.3 (Optional) Configuring Web System Parameters

Context

The device can function as an HTTPS server and use the data encryption, identity authentication, and message integrity check mechanisms of the SSL protocol to ensure secure data transmission between the device and users. Users can securely access a remote device on web pages.

The device has the web system function enabled before delivery and provides a default SSL policy. The web page file contains the SSL certificate. Therefore, you do not need to perform the following operations.

For security purposes, you are advised to obtain a new digital certificate from a CA and manually configure an SSL policy. For details, see Configuring the Device as an HTTPS Server in the *Huawei AR Series Access Routers Configuration Guide - Security*. The details are not mentioned here.

Procedure

Step 1 Run **system-view**

The system view is displayed.

Step 2 (Optional) Run **set insecure-protocol enable**

Insecure management protocols HTTP and Telnet are allowed to be used.

By default, insecure management protocols HTTP and Telnet can be used except AR161EW, AR161EW-M1, AR169EW, AR169EGW-L, and AR2204XE. By default, insecure management protocols HTTP and Telnet cannot be used on the AR161EW, AR161EW-M1, AR169EW, AR169EGW-L, and AR2204XE.

Step 3 Run **http server enable**

The web system function is enabled.

By default, the web system function is enabled on the device.

Step 4 Run **http server-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* }

The source IP address of the web system is configured.

By default, the source IP address of the web system is not configured.

If the source IP address is not specified for the web system, the device selects a source IP address according to routing entries to send packets. Specify an interface in stable state, such as a loopback interface, as the source interface. Before specifying a source interface, ensure that clients have reachable routes to the source interface. Otherwise, the configuration will fail.

Step 5 Run **http secure-server port** *port-number*

The port number of the HTTPS server is configured.

 Copyright © Huawei Technologies Co., Ltd.

The default port number of the HTTPS server is 443.

If the default port number is used, attackers may access this port continuously, consuming bandwidth resources and degrading security performance of the server. As a result, authorized users cannot access the device. If the default port number is used by another service, users cannot log in to the device through the web system.

Step 6 Run **http secure-server manager-port** *port-number*

The management port of the HTTPS server is enabled and the management port number is set.

By default, the management port of the HTTPS server is disabled.

You can run this command to enable the management port of the HTTPS server and set the management port number, and then can manage the router.

NOTE

Only users at level 3 and higher levels can log in to the web platform through the management port.

Step 7 Run **http server max-online-users** *max-online-users*

The maximum number of concurrent online users in the web system is set.

By default, the maximum number of concurrent online users in the web system is 5.

You can configure the maximum number of concurrent online users in the web system to restrict the number of users who access the web system at the same time.

Step 8 Run **http timeout** *timeout*

The HTTPS session timeout interval is set.

By default, the HTTPS session timeout interval is 10 minutes.

By default, only five users can concurrently log in to the device through the web system. If a web user logs in to the device but does not perform any operations for a long time, the user occupies web channel resources and other users may fail to log in to the device. You can set a proper HTTPS session timeout interval so that web channel resources can be released in a timely manner.

Step 9 Configure ACL-based access control for the web system.

1. Run **acl** [**number**] *acl-number*

   A numbered ACL is created and the ACL view is displayed.

2. Configure an ACL rule.

   The command for configuring rules for a basic ACL differs from that for configuring rules for an advanced ACL.

   – For a basic ACL, run **rule** [*rule-id*] { **deny** | **permit** } [**source** { *source-address source-wildcard* | **any** } | **vpn-instance** *vpn-instance-name* | [**fragment** | **none-first-fragment**] | **logging** | **time-range** *time-name*] *

- For an advanced ACL, run **rule** [*rule-id*] { **deny** | **permit** } **ip** [**destination** { *destination-address destination-wildcard* | **any** } | **source** { *source-address source-wildcard* | **any** } | **logging** | **time-range** *time-name* | **vpn-instance** *vpn-instance-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | [**fragment** | **none-first-fragment**]] *

3. Run **quit**

   Return to the system view.

4. Run **http acl** *acl-number*

   An ACL is configured for the HTTPS server.

   By default, no ACL is configured for the HTTPS server, that is, web users using any clients can establish HTTPS connections with the device.

Step 10 Run **http server permit interface** { *interface-type interface-number* } &<1-5>

An interface is configured to allow clients to access the web system.

By default, all interfaces on the device allow clients to access the web system.

To prevent unauthorized clients from accessing the web system through an interface, you can run this command to specify an interface that allows clients to access the web system.

NOTE

You can only run the **http server permit interface** command to configure physical interfaces and VLANIF interfaces.

In the factory default settings of the device, users can only access the web platform through management interfaces. For example, when the management interface of the device is GE0, the http server permit interface GigabitEthernet0/0/0 command is contained in the factory default settings of the device.

Step 11 Run **set web login-style** { **professional** | **simple** }

The edition for web platform login to the router is set.

By default, the EasyOperation edition is used for web platform login to a router.

NOTE

Only the AR100&AR120&AR150&AR160&AR200 series routers support this step.

----End

10.4.4 (Optional) Setting the Storage Directory of the Logo Image on the Web Page

Context

The device supports customization of the logo image on the web page. You can change the logo image based on actual requirements so that the logo image on the web page is more beautiful.

The logo image must be stored using the required file name and size in the subdirectory for storing the logo image. After the storage directory of the logo

 Copyright © Huawei Technologies Co., Ltd.

image on the web page is set, the device automatically reads the file under the directory and changes the logo image on the web page.

Store three files with different pixel sizes of the required logo image in the created subdirectory, and name them as required. Name the image with the pixel size 16x16 **logo1.png**, the image with the pixel size 21x22 **logo2.png**, and the image with the pixel size 44x44 **logo3.png**.

Procedure

Step 1 Run **mkdir** *directory*

A subdirectory is created for storing the logo image under the directory **logo-path** of the default working directory on the device.

Step 2 Run **system-view**

The system view is displayed.

Step 3 Run **set logo-path** *subpathname*

The storage directory of the logo image on the web page is set.

By default, the storage directory of the Huawei logo image is used.

----End

10.4.5 Creating a Web System Account

Context

You can log in to the web system only after entering the correct user name and password. The network administrator can configure the user name, password, level, and service type to create a web system user. After the configuration is complete, you can log in to the web system using the configured web system account.

Procedure

Step 1 Run **system-view**

The system view is displayed.

Step 2 Run **aaa**

The AAA view is displayed.

Step 3 Run **local-user** *user-name* **password irreversible-cipher** *password*

A web system user name and password are configured.

By default, the system has a local user whose user name is **admin**. The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

Step 4 Run **local-user** *user-name* **service-type http**

 Copyright © Huawei Technologies Co., Ltd.

The service type is set to HTTP.

By default, the service type of the local user **admin** is HTTP.

Step 5 Run **local-user** *user-name* **privilege level** *level*

The user level is configured.

By default, the level of the local user **admin** is **15**, that is, the local user is a super administrator.

NOTE

If the level of a user is 0 or no level is configured for the user, the user does not have the right to log in to the web system. The mapping between user levels and users is as follows:

- If the user level is 1, the user is a common administrator.
- If the user level is 2, the user is an enterprise administrator.
- If the user level is 3 to 15, the user is a super administrator.

Step 6 Run **quit**

Return to the system view.

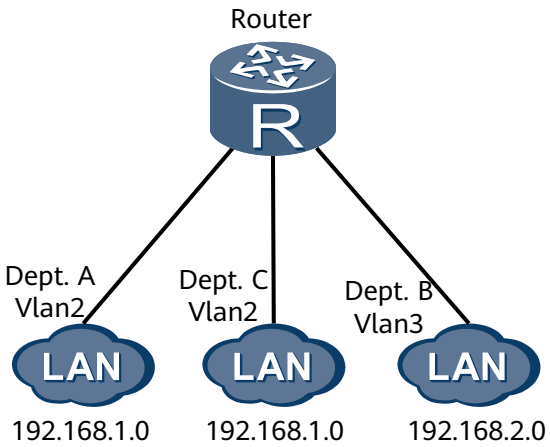
----End

10.4.6 Logging In to the Web System

Context

As shown in **Figure 10-1**, a PC connects to a router through an IP network. After configuring the router's IP address, web system parameters, and a web system account, you can configure and manage the router on the PC through the web system.

Figure 10-1 Web system networking

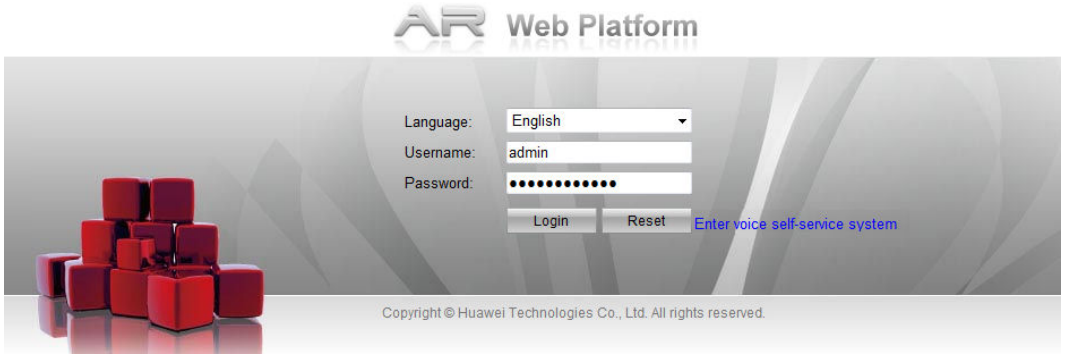


Procedure

Step 1 Open the browser on the PC. Windows IE8.0 is used in this example. Enter https://*ip address* in the address box and press **Enter**. The web system login page is displayed, as shown in **Figure 10-2**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 10-2 Web system login page



NOTE

You can use the web mode to configure voice services only when the device works in PBX mode.

If the device supports the voice self-service system, you can log in to the voice self-service system using either of the following methods:

- On the web platform, click **Enter voice self-service system**.
- Before logging in to the voice self-service system, run the **self-service-http-server** command in the voice view to access the self-service HTTP server configuration view, and then run the **self-service http secure-server enable** command to enable the self-service HTTPS server. You can enter **https://ip address:1443/professional/user/login.html** in the address box to access the voice self-service system. In the configuration view of the self-service HTTPS server, you can run the **self-service http secure-server port** command to change the port number of the self-service HTTPS server. The default port number is 1443.

Step 2 Enter login information.

1. Select a language.

   Currently, the web system supports English and Chinese, and automatically uses a language based on the browser.

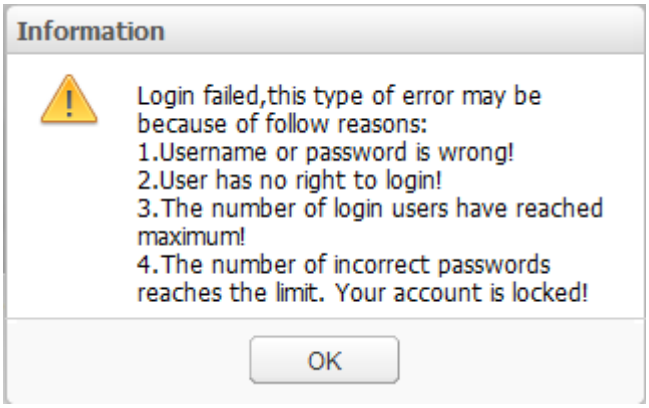
2. Enter the user name and password.

   The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

3. Click **Login**.

   The system displays a message about login failure in situations shown in **Figure 10-3**.

Figure 10-3 Login failure



Check the cause of the login failure based on the prompt message. If the number of incorrect password attempts reaches the upper limit, the current account will be locked. By default, a locked account is automatically unlocked after 5 minutes.

NOTE

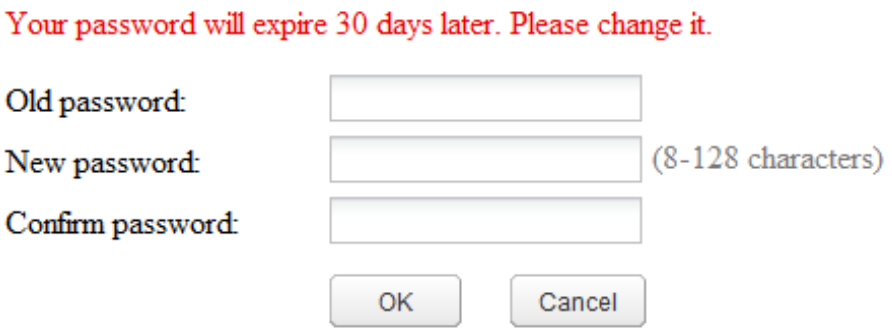
After a user logs in, the web system automatically displays the last login time, IP address, and login mode of the user.

Step 3 Change the login password.

The system asks you to change the password in the following situations, as shown in **Figure 10-4**.

- If the login password expires, the system forcibly requires you to change the password.
- If you log in to the system for the first time after the password is changed by another user, the system forcibly requires you to change the password.
- If you log in to the system within the password expiration notification period, the system notifies you of the password expiration time and advises you to change the password.

Figure 10-4 Password change page



 Copyright © Huawei Technologies Co., Ltd.

NOTE

- If the parameters are marked with a red asterisk (*), the system forcibly requires you to change the password. After changing the password, click **OK**. If the password is changed successfully, the system displays the message "Your password has been modified successfully". Click **OK**. The login page is displayed. If you do not change the password, click **Cancel**. The login page is displayed and you cannot log in to the web system.
- If the parameters are not marked with a red asterisk (*), the system asks you to change the password. After changing the password, click **OK**. If the password is changed successfully, the system displays the message "Your password has been modified successfully". Click **OK**. The login page is displayed. If you do not change the password, click **Cancel**. The **Device Information** page is displayed.

Step 4 Click **Logout** in the upper right corner of the page to return to the login page.

Step 5 If you do not perform any operations within a period (10 minutes by default) after logging in to the web system, the system automatically logs you out. Click **OK** to return to the login page.

----End

10.4.7 Verifying the Configuration

Context

After completing the configuration, run the following commands in any view on the CLI to check information about online web users and the web system.

Procedure

Step 1 Run the **display http server** command to check information about the web system.

Step 2 Run the **display http user** [**username** *username*] command to check information about online web users.

----End

10.5 Configuration Examples for Web System Login

This section provides an example for configuring device login through the web system.

10.5.1 Example for Configuring Device Login Through the Web System

Networking Requirements

As shown in **Figure 10-5**, there are reachable routes between the device and PC. It is required that the device be managed and maintained through the web system.

Figure 10-5 Networking diagram for configuring device login through the web system



Configuration Roadmap

The configuration roadmap is as follows:

1. Log in to the device through the console port.
2. Configure a management IP address for the device.
3. Create a web system account.
4. Enable the web system function.
5. Log in to the web system.

Procedure

Step 1 Log in to the device through the console port. For details, see Example for Configuring First Login Through the Console Port.

Step 2 Configure a management IP address for the device.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 0/0/0
[Huawei-GigabitEthernet0/0/0] ip address 10.1.1.1 24
[Huawei-GigabitEthernet0/0/0] quit
```

Step 3 Configure a web user.

```
[Huawei] aaa
[Huawei-aaa] local-user admin password irreversible-cipher Helloworld@6789
[Huawei-aaa] local-user admin privilege level 15
[Huawei-aaa] local-user admin service-type http
[Huawei-aaa] quit
```

NOTE

Before configuring a web user, you can run the **display this** command in the AAA view to check user names of local users. Ensure that the user name of the configured web user does not conflict with that of an existing local user; otherwise, the new web user may overwrite the existing local user.

Step 4 Configure the web system.

Enable the web system function.

```
[Huawei] http server enable
  This operation will take several minutes, please wait.....................................................
Info: Succeeded in starting the HTTP server
[Huawei] quit
```

Step 5 Log in to the web system.

Open the web browser on the PC, enter **https://10.1.1.1** in the address box, and press **Enter**. The web system login page is displayed, as shown in **Figure 10-6**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 10-6 Web system login page



Enter the web user name and password, and click **Login** or press **Enter**. The web system homepage is displayed.

Step 6 Verify the configuration.

After the configuration is complete, you can successfully log in to the device through the web system.

Run the **display http server** command on the device to check the SSL policy name and HTTPS server status.

```
<Huawei> display http server
  HTTP server status    : Enabled       (default: disable)
  HTTP server port      : 80            (default: 80)
  HTTP timeout interval : 10            (default: 10 minutes)
  Current online users  : 0
  Maximum users allowed : 5
  HTTPS server status   : Enabled       (default: disable)
  HTTPS server port     : 443           (default: 443)
  HTTPS SSL Policy      :
```

----End

Configuration Files

Configuration file of the device

```
#
 pki-realm default
#
aaa
 local-user admin password irreversible-cipher %^%#R!d3>ji-.u1+N2gSK>3&2P1AM6jfU:"x/3g[5U,lvqP
+sf=70+%^E7,,SF7+%^%#
 local-user admin privilege level 15
 local-user admin service-type http
#
interface GigabitEthernet0/0/0
 ip address 10.1.1.1 255.255.255.0
#
 http server enable
#
return
```

10.6 Common Misconfigurations

This section describes common faults caused by incorrect configurations and provides the troubleshooting procedure.

10.6.1 Device Login Through the Web System Fails

Symptom

The device cannot be logged in through the web system.

Procedure

Step 1 Check whether the device and client can ping each other.

Access the Windows Command Prompt and run the **ping** command to check whether the PC and device are reachable to each other. If the system displays "Request time out", the target device is unreachable.

Check whether the physical interface that receives ping packets is blocked. If the physical interface is not blocked, check whether the correct gateway address is configured on the device, and whether the device and PC are on the same network segment. If they are on different network segments, run the **ip address** *ip-address* { *mask* | *mask-length* } command in the interface view to reconfigure the management IP address of the device in the target network segment.

Step 2 Check whether the login address is correct.

Check the *IP address:port* in https://*IP address* entered in the address box of the browser. If the IP address is incorrect, enter the correct one to log in to the web system.

Step 3 Check whether the HTTPS service is enabled.

Run the **display this** command in the system view to check whether the **http secure-server enable** configuration exists. If not, the HTTPS service is disabled. Run the **http secure-server enable** command in the system view to enable the HTTPS service.

Step 4 Check whether the number of online web users reaches the maximum.

Run the **display http server** command in any view to check the maximum number of access users allowed by the web system. Run the **display http user** command in any view to check the number of online web users. If the number of online web users reaches the maximum number of access users allowed by the web system, you can log in to the device only after other users go offline.

Step 5 Check whether the IP address is correctly configured.

Run the **display this** command in the interface view to check whether the configured IP address is correct. If not, run the **ip address** *ip-address* { *mask* | *mask-length* } command in the interface view to reconfigure the management IP address of the device.

Step 6 Check whether the web user is correctly configured.

Run the **display this** command in the AAA view to check whether the web user is correctly configured.

- If the **local-user** *user-name* **password irreversible-cipher** *password* configuration exists, an AAA user named *user-name* is configured.

 Copyright © Huawei Technologies Co., Ltd.

- If the **local-user** *user-name* **privilege level** *level* configuration exists, the level of the user *user-name* is *level*.
- If the **local-user** *user-name* **service-type http** configuration exists, the service type of the user *user-name* is HTTP.

If any of the preceding configurations does not exist, run the following commands in the AAA view:

- Run the **local-user** *user-name* **password irreversible-cipher** *password* command to configure the web user name and password.
- Run the **local-user** *user-name* **privilege level** *level* command to set the web user level.
- Run the **local-user** *user-name* **service-type http** command to set the web user's service type to HTTP.

Step 7 Check whether access control on web users is configured on the device.

Run the **display this** command in the system view to check whether the **http acl** *acl-number* configuration exists. If so, record the value of *acl-number*.

Run the **display acl** *acl-number* command in any view to check whether the web user's client IP address is denied in the ACL. If so, run the **undo rule** *rule-id* command in the ACL view to delete the deny rule, and run the corresponding command to modify the ACL so that the web user's client IP address is allowed.

----End

10.6.2 The Web System Page Is Not Completely Displayed After Successful Device Login Through the Web System

Symptom

After successful device login through the web system, the web system page is not completely displayed, or only several options are displayed.

Procedure

Step 1 Check whether the web user level is too low.

If the user level is 1, the user is a common administrator and can only access **Device Information** and change the password in **User Management**. If the user level is 2, the user is an enterprise administrator and has most operating rights in the web system. If the user level is 3 to 15, the user is a super administrator and has all operating rights in the web system.

Run the **display this** command in the AAA view to check the web user level. If the value of *level* is too small in the **local-user** *user-name* **privilege level** *level* configuration, some functions cannot be displayed in the web system. Run the **local-user** *user-name* **privilege level** *level* command in the AAA view to set the web user level to 3 or higher so that the web user has all operating rights in the web system.

Step 2 Check whether the device version is correct.

Run the **display version** command in any view to check the device version. If the value of *Version* is too small in the **VRP (R) software, Version** *Version*

 Copyright © Huawei Technologies Co., Ltd.

configuration, the device does not support some functions in the web system. Upgrade the device to a proper version.

----End

10.7 FAQ About Web System Login

This section describes common problems you may encounter during the configuration and provides the solutions to these problems.

10.7.1 Does the AR Series Support the Web NMS?

The AR series supports the web network management system (NMS) from V200R002C01. You can use the web network management system to manage and maintain AR series.

10.7.2 How Do I Configure the Web User Level?

Run the **local-user** *user-name* **privilege level** *level* command in the AAA view to set the web user level.

- If the user level is 1, the user is a common administrator and can only access **Device Information** and change the password in **User Management**.
- If the user level is 2, the user is an enterprise administrator and has most operating rights in the web system.
- If the user level is 3 to 15, the user is a super administrator and has all operating rights in the web system.

You are advised to set *level* to 3 or higher.

10.7.3 What Should I Do If I Forget the Web System Login Password?

If you forget or want to change the web system login password, log in to the device through the console port, Telnet, or STelnet and set a new password after login.

NOTE

Telnet has security vulnerabilities. You are advised to log in to the device using STelnet V2.

Set the password to **Huawei@123** for the user **admin123**. The configuration is as follows:

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] local-user admin123 password irreversible-cipher Huawei@123
[Huawei-aaa] local-user admin123 service-type http
[Huawei-aaa] local-user admin123 privilege level 15
[Huawei-aaa] return
<Huawei> save
```

10.7.4 What Is the Default Login Password?

 Copyright © Huawei Technologies Co., Ltd.

The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

NOTE

For security purposes, you are advised to change the default password for the device.

10.7.5 What Should I Do If the Account Is Locked?

By default, a locked account is automatically unlocked after 5 minutes. You can wait until the account is automatically unlocked, and enter the correct user name and password to log in to the device again.

You can also log in to the device using the CLI mode when the account is locked, and run the **local-user** *user-name* **state active** command in the AAA view to unlock the account.

10.7.6 How Do I Obtain the Web Page File?

The system software contains the web page file. After new system software is loaded to the device, the web page file **web.zip** is directly decompressed from the system software and saved to the memory.

10.7.7 How Do I Change the Port Number for Web System Login?

Procedure

You can run the **http secure-server port** *port-number* command in the system view to reconfigure the port number of the HTTPS server.

More Information

- Changing the port number of the HTTPS service forces all online users to go offline. Therefore, exercise caution when performing this operation.
- The default port number of the HTTPS server is 443. If you access and control the device through the web platform, you do not need to specify the port number. If the default port number is used, attackers may access this port continuously, consuming bandwidth resources and degrading security performance of the server. As a result, authorized users cannot access the device. If the default port number is used by another service, users cannot log in to the device through the web platform. This command allows you to set another port number for the HTTPS service to avoid such attacks.

 Copyright © Huawei Technologies Co., Ltd.

11 File Management

About This Chapter

This chapter provides information about file management. This information includes an overview, descriptions, and other details related to file management.

11.1 Overview of the File System

11.2 File Management Modes
The device supports multiple file management modes. You can choose a proper file management mode based on service and security requirements.

11.3 Licensing Requirements and Limitations for File Management
This section provides the configuration precautions of file management.

11.4 Local File Management
You can manage the local files on the device through a console port or using Trivial File Transfer Protocol (TFTP), File Transfer Protocol (FTP), or Secure File Transfer Protocol (SFTP).

11.5 File Management on Other Devices

11.6 Configuration Examples for File Management

11.7 Troubleshooting System Startup

11.8 FAQ About File Management
This section describes common problems that may occur during the configuration and their solutions.

11.1 Overview of the File System

File System

The file system manages files and directories on storage media. In the file system, users can create, delete, modify, and rename a file or a directory, and view contents of a file.

 Copyright © Huawei Technologies Co., Ltd.

Storage Medium

The AR100&AR120&AR150&AR160&AR200&AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204E-D-27GE, AR2204-24GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-48GE-P, AR2204E, AR2204E-D, AR2204-51GE, AR2204-51GE-R, AR2220L-DC, AR2220L-AC and AR3670 support the flash memory and USB flash drive. The AR2220-AC, AR2220-DC, AR2220E, AR2240C support the flash memory, hard disk and USB flash drive. The AR2204, AR2240 and AR3260 (using SRU40, SRU60, SRU80, SRU100, SRU100E, SRU200E, SRU200 and SRU400) support the flash memory, Micro SD card, and USB flash drive. The AR2240, AR2204XE-DC and AR2204XE support the Micro SD card and USB flash drive.

NOTE

- A USB flash drive is mainly used for USB-based deployment or system file loading. If the USB flash drive contains activated system software or patch software, the USB flash drive is a key component of the system and cannot be removed. The USB flash drive must use the FAT32 format. Set the format to FAT32 (format the USB flash drive) before using the USB flash drive.
- The external memory is used to store logs. Do not store software packages, configuration files, license files, and patch files in the external memory.

Naming Rules for Files

The file name is a string of 1 to 64 characters without spaces. Only names of the following files are case-sensitive:

- Files in the built-in storage medium on the AR100&AR120 series
- Files in the built-in storage medium on the AR161&AR169&AR161G-L&AR161G-Lc&AR169G-L&AR169EGW-L&AR169-P-M9&AR169W-P-M9&AR169RW-P-M9 of the AR160 series
- Files in the built-in storage medium on the AR1200C of the AR1200 series
- Files in the built-in storage medium on the AR2204-27GE&AR2204E-D-27GE&AR2204-27GE-P&AR2204-51GE-P&AR2204-51GE-R&AR2204E&AR2204E-D of the AR2200 series
- Files in the built-in storage medium on the AR3600 series

If names of files in the storage medium on the device are case-sensitive, you need to enter case-sensitive file names when operating the files in the FTP client view or SFTP client view.

The file name formats are as follows:

- File name

  A file resides in the current working directory if the file name is in this format.
- Drive + Path + File name

  This file name format uniquely identifies files in specified paths.

  drive is the storage medium and is named as:
  - sd1: root directory of the Micro SD card on the master SRU.
  - flash: root directory of the flash memory on the master SRU.
  - slave#sd1: root directory of the Micro SD card on the slave SRU.
  - slave#flash: root directory of the flash memory on the slave SRU.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Only the AR3200 series supports dual SRUs.

In the file name, **path** indicates the directory and subdirectory. The directory name is case-insensitive. Spaces and the following characters cannot be used in the directory name: ~ * / \ : ' "

Paths are either absolute or relative.

- **flash:/my/test/** is an absolute path.
- **/selftest/** is related to the root directory and indicates the **selftest** directory in the root directory.
- **selftest/** is related to the current working directory and indicates the **selftest** directory in the current working directory.

For example, in the **dir flash:/my/test/mytest.txt** command, **flash:/my/test/** is an absolute path.

Run the **dir test/mytest.txt** command to find the **mytest.txt** file from a directory related to the current working directory (**flash:/my/** for example).

NOTE

- In the file operation command format, **filename** indicates the file name.
- In the file operation command format, **directory** indicates the path (**drive + path**).

11.2 File Management Modes

The device supports multiple file management modes. You can choose a proper file management mode based on service and security requirements.

Users can log in to a device or use the File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), or Secure File Transfer Protocol (SFTP) mode to manage files.

Table 11-1 describes file management modes and their advantages and disadvantages.

Table 11-1 File management modes

Mode	Usage Scenario	Advantage	Disadvantage
Log in to the device	In the scenario of managing storage media, directories, and files, log in to the device through the console port, Telnet, or STelnet. This login mode is mandatory for storage medium management.	You can log in to the device directly to manage storage media, directories, and files.	Only files on the local device can be managed. File transfer is not supported.

 Copyright © Huawei Technologies Co., Ltd.

Mode	Usage Scenario	Advantage	Disadvantage
FTP	The FTP mode is applicable to the file transfer scenario with low network security requirements. The FTP mode is widely used in version upgrade.	• The FTP mode is easy to configure and supports file transfer and operations on directories. • The FTP mode supports file transfer between two file systems. • The authorization and authentication functions are provided.	In FTP mode, data is transmitted in plain text, causing security risks.
TFTP	On the LAN, the TFTP mode can be used to load or upgrade versions online. The TFTP mode is applicable to the environment without complicated interactions between a client and a server.	Compared with FTP mode, TFTP mode consumes less memory usage.	• The TFTP mode supports only file transfer. • In TFTP mode, data is transmitted in plain text, causing security risks, and no authorization or authentication function is provided.
SFTP	The SFTP mode is applicable to the scenario with high network security requirements. The SFTP mode is widely used in log download and file backup.	• Data is encrypted and protected. • The SFTP mode supports file transfer and operations on directories.	Configurations are complicated.

The device can function as a server or client to manage files.

- When the device functions as a server, you can access the device on a client to manage files on the device and transfer files between the device and the client.
- When the device functions as a client, you can use the device to manage files on other devices and transfer files between the device and other devices.

 Copyright © Huawei Technologies Co., Ltd.

11.3 Licensing Requirements and Limitations for File Management

This section provides the configuration precautions of file management.

Involved Network Elements

None

Licensing Requirements

File management is a basic feature of a router and is not under license control.

Feature Limitations

None

11.4 Local File Management

You can manage the local files on the device through a console port or using Trivial File Transfer Protocol (TFTP), File Transfer Protocol (FTP), or Secure File Transfer Protocol (SFTP).

Context

NOTICE

When downloading files to the device or performing other operations on the device, ensure that the power supply of the device is working properly; otherwise, the downloaded file or the file system may be damaged. As a result, the storage medium on the device may be damaged or the device cannot be properly started.

11.4.1 Logging In to the Device to Manage Files

Pre-configuration Tasks

Before logging in to the device to manage files, complete the following tasks:

- Ensure that routes are reachable between the terminal and the device.
- Ensure that a user have logged in to the device using a terminal.

Configuration Process

After a user logs in to the device on a terminal, the user can perform operations on storage media, directories, and files.

Users can perform the following operations in any sequence and select one or more action items according to requirements.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

- **Perform operations on directories.**

  Table 11-2 Performing operations on directories

Operation	Command	Description
Display the current directory.	**pwd**	-
Change the current directory.	**cd** *directory*	-
Display files and subdirectories in a specified directory.	**dir** [**/all**] [*filename* | *directory*]	-
Create a directory.	**mkdir** *directory*	-
Delete a directory.	**rmdir** *directory*	• The directory to be deleted must be empty. • A deleted directory and its files cannot be restored from the recycle bin.

- **Perform operations on files.**

  Table 11-3 Performing operations on files

Operation	Command	Description
Display the file content.	**more** [**/binary**] *filename* [*offset*] [**all**]	-
Copy a file.	**copy** *source-filename destination-filename*	• Before copying a file, ensure that the storage space is sufficient for the file. • If the target file has the same name as an existing file, the system prompts you whether to overwrite the existing file.
Move a file.	**move** *source-filename destination-filename*	If the target file has the same name as an existing file, the system prompts you whether to overwrite the existing file.

 Copyright © Huawei Technologies Co., Ltd.

Operation	Command	Description
Rename a file.	**rename** *old-name new-name*	-
Compress a file.	**zip** *source-filename destination-filename*	-
Decompress a file.	**unzip** *source-filename destination-filename*	-
Delete a file.	**delete** [**/unreserved**] [**/force**] { *filename* | *devicename* }	This command cannot delete a directory. **NOTICE** In this command, **/unreserved** indicates that the file cannot be restored.
Restore a file.	**undelete** { *filename* | *devicename* }	If you run the **delete** command without the **/unreserved** keyword, the file is moved to the recycle bin. You can run this command to restore the files in the recycle bin.
Remove a file from the recycle bin.	**reset recycle-bin** [*filename* | *devicename*]	To delete a file permanently, remove the file from the recycle bin.
Enter the system view.	**system-view**	To perform multiple operations at one time, run the **execute** *batch-filename* command in the system view. The batch files must be stored in the storage medium first.
Execute batch files.	**execute** *batch-filename*	

- **Perform operations on storage media.**
  - When the file system fault cannot be rectified or the data on the storage medium is unnecessary, you can format the storage medium.

    NOTICE

    When a storage medium is formatted, data on the storage medium is cleared and cannot be restored. Therefore, exercise caution when you format a storage medium.

  - When a storage medium is not required, remove it safely to prevent files on the device from being damaged.

 Copyright © Huawei Technologies Co., Ltd.

Table 11-4 Performing operations on storage media

Operation	Command	Description
Format a storage medium.	**format** *drive*	If the storage medium is still unavailable after it is formatted, a physical exception occurs.
Remove a storage medium.	**remove** *drive*	Run this command to remove a storage medium safely to ensure that files stored in the device are not damaged.

- **Configure the notification mode of the file system.**

  When a user performs operations that may cause data loss or damage on a device, the system generates notifications or alarms. Users can configure the notification mode of the file system.

  Table 11-5 Configuring the notification mode of the file system

Operation	Command	Description
Enter the system view.	**system-view**	-
Configure the notification mode of the file system.	**file prompt** { **alert** | **quiet** }	The default notification mode is **alert**. **NOTICE** If the notification mode is set to **quiet**, the system does not provide notifications when data is lost caused by user misoperations such as deleting files. Therefore, this notification mode must be used with caution.

----End

11.4.2 Managing Files When the Device Functions as a TFTP Server

Users can use the TFTP protocol to manage files, for example, performing version upgrade.

Pre-configuration Tasks

Before managing files using TFTP, complete the following task:

- Configure reachable routes between the TFTP server and TFTP client.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Process

NOTE

The TFTP protocol has security risks; therefore, SFTPv2 is recommended for file management.

Table 11-6 describes the configuration process for managing files using TFTP.

Table 11-6 Managing files using TFTP

No.	Task	Description	Remarks
1	**Configuring the TFTP Server Function and Related Parameters**	Enable the TFTP server function and configure the following parameters: port number, working directory, and packet timeout period.	-
2	**Uploading or Downloading Files Using TFTP**	Access the device from a TFTP client.	-

Procedure

- **Configure the TFTP server function and related parameters.**

  Table 11-7 Configuring the TFTP server function and related parameters

Procedure	Command	Description
Enter the system view.	**system-view**	-

Procedure	Command	Description
(Optional) Configure a port number for the TFTP server.	**tftp server port** *port-number*	By default, the port number of the TFTP server is 69. **NOTE** Ensure that the TFTP service is disabled before you run this command. If the TFTP service is enabled, the port number of the TFTP server cannot be changed. Run the **undo tftp server enable** command first to disable the TFTP service and then change the port number. When the port number of the TFTP server is 69, a TFTP client can connect to the TFTP server without the need to specify a port number. When the port number of the TFTP server is not 69, you need to specify a port number for the TFTP client before it can connect to the TFTP server, and the specified client port number must be the same as the server port number.
(Optional) Configure a packet timeout period for the TFTP server.	**tftp server timeout** *timeout-second*	By default, the packet timeout period of a TFTP server is 5 seconds. The TFTP server will resend a packet if it does not receive any response within the specified timeout period. If the packet times out three times, the TFTP server disconnects the TFTP connection.
Configure a working directory for the TFTP server.	**set default tftp-directory** *directory*	By default, no working directory is configured for the TFTP server.

 Copyright © Huawei Technologies Co., Ltd.

Procedure	Command	Description
Enable the TFTP server function.	**tftp server enable**	By default, the TFTP server function is disabled. Configure a working directory for the TFTP server before you run this command. **NOTE** After file operations between the client and device are complete, run the **undo tftp server enable** command to disable the TFTP server function in a timely manner to protect device security.

- **Upload or download files using TFTP.**
  - The device can communicate with a terminal that functions as the TFTP client. In this case, install and run TFTP software on the terminal before performing TFTP operations. For details on how to use TFTP software, see the help document of the third-party TFTP software.
  - The device can communicate with another device that functions as the TFTP client. In this case, you can run the following commands on the TFTP client.

Procedure	Command	Description
Run the TFTP command to manage files.	**tftp** [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *tftp-server* [**public-net** | **vpn-instance** *vpn-instance-name*] { **get** | **put** } *source-filename* [*destination-filename*]	Select one of them based on the address type. • **get**: download files. • **put**: upload files. **NOTE** You cannot access a TFTP client with an IPv6 address.

----End

Verifying the Configuration

- Run the **display tftp-server status** command to check the TFTP server information.

11.4.3 Managing Files When the Device Functions as an FTP Server

Users can connect the local terminal to a remote device to manage files using FTP. FTP is widely used for file service operations such as version upgrade.

 Copyright © Huawei Technologies Co., Ltd.

Pre-configuration Tasks

Before connecting to the FTP server to manage files, complete the following tasks:

- Ensure that routes are reachable between the terminal and the device.
- Ensure that the terminal functions as the FTP client.

Configuration Process

NOTE

The FTP protocol will bring risk to device security. The SFTPv2 mode is recommended.

Table 11-8 describes the procedure for managing files when the device functions as an FTP server.

Table 11-8 Managing files when the device functions as an FTP server

No.	Task	Description	Remarks
1	**Set FTP server parameters**	Configure FTP server parameters including the port number, source address, and timeout duration.	The three steps can be performed in any sequence.
2	**Configure local FTP user information**	Configure local FTP user information including the service type, user level, and authorized directory.	The three steps can be performed in any sequence.
3	**(Optional) Configure the FTP ACL**	Configure the ACL rule and FTP basic ACL to improve FTP access security.	The three steps can be performed in any sequence.
4	**Connect to the device using FTP**	Connect to the device using FTP from the terminal.	-

Default Parameter Settings

Table 11-9 Default parameter settings

Parameter	Default Value
FTP server function	Disabled
Listening port number	21
FTP user	No local user is created.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

- **Set FTP server parameters.**

Table 11-10 Setting FTP server parameters

Operation	Command	Description
Enter the system view.	**system-view**	-
(Optional) Specify a port number for the FTP server.	**ftp** [**ipv6**] **server port** *port-number*	The default port number is 21. If a new port number is configured, the FTP server disconnects from all FTP clients and uses the new port number to listen to connection requests. Attackers do not know the port number and cannot access the listening port of the FTP server.
Enable the FTP server function.	**ftp** [**ipv6**] **server enable**	By default, the FTP server function is disabled.
(Optional) Configure the source address of the FTP server.	**ftp server-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* }	After the source address of the FTP server is configured, incoming and outgoing packets are filtered, ensuring the device security. After the source address of the FTP server is configured, you must enter the source address to log in to the FTP server.
(Optional) Configure the timeout duration of the FTP server.	**ftp** [**ipv6**] **timeout** *minutes*	By default, the idle timeout duration is 30 minutes. During the timeout duration, if no operation is performed on the FTP server, the FTP client disconnects from the FTP server automatically.
(Optional) Specify physical interfaces on the FTP server to which clients can connect.	**ftp server permit interface** { *interface-type interface-number* } &<1-5>	By default, clients can connect to all the physical interfaces on the FTP server.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- If the FTP service is enabled, the port number of the FTP service cannot be changed. To change the port number, run the **undo ftp** [**ipv6**] **server** command to disable the FTP service first.
- After operations on files are complete, run the **undo ftp** [**ipv6**] **server** to disable the FTP server function to ensure the device security.

- **Configure local FTP user information.**

  Before performing operations on files using FTP, configure the local user name and password, service type, and authorized directory on the FTP server.

  Table 11-11 Configuring local FTP user information

Operation	Command	Description
Enter the system view.	**system-view**	-
Enter the AAA view.	**aaa**	-
Configure the local user name and password.	**local-user** *user-name* **password irreversible-cipher** *password*	-
Configure the local user level.	**local-user** *user-name* **privilege level** *level*	**NOTE** The user level must be set to **3** or higher to ensure successful connection establishment.
Configure the service type for local users.	**local-user** *user-name* **service-type ftp**	By default, a local user can use any access type.
Configure an authorized directory.	**local-user** *user-name* **ftp-directory** *directory*	By default, the FTP directory of a local user is empty. When multiple FTP users use the same authorized directory, you can use the **set default ftp-directory** *directory* command to configure a default directory for these FTP users. In this case, you do not need run the **local-user** *user-name* **ftp-directory** *directory* command to configure an authorized directory for each user.

- **(Optional) Configure an ACL for the FTP server.**

 Copyright © Huawei Technologies Co., Ltd.

An ACL is composed of a list of rules such as the source address, destination address, and port number of packets. ACL rules are used to classify packets. After these rules are applied to routing devices, the routing devices determine the packets to be received and rejected.

Users can configure a basic ACL to allow only specified clients to connect to the FTP server.

The ACL rules are as follows:

- When **permit** is used in the ACL rule, devices that match the ACL rule can establish an FTP connection with the local device.
- When **deny** is used in the ACL rule, devices that match the ACL rule cannot establish FTP connections with the local device.
- When the ACL rule is configured but packets from devices do not match the rule, other devices cannot establish FTP connections with the local device.
- When the ACL contains no rule, any device can establish FTP connections with the local device.

Table 11-12 (Optional) Configuring an ACL for the FTP server

Operation	Command	Description
Enter the system view.	**system-view**	-
Enter the ACL view.	**acl** [**number**] *acl-number*	**NOTE** FTP supports only basic ACLs (2000-2999).
Configure the ACL rule.	**rule** [*rule-id*] { **deny** | **permit** } [**source** { *source-address source-wildcard* | **any** } | **vpn-instance** *vpn-instance-name* | [**fragment** | **none-first-fragment**] | **logging** | **time-range** *time-name*] *	-
Return to the system view.	**quit**	-
Configure a basic ACL for the FTP server.	**ftp** [**ipv6**] **acl** *acl-number*	-

- **Connect to the device using FTP.**

  Users can use the Windows CLI or third-party software to connect to the device from a terminal using FTP. The following describes how to connect to the device using commands in the Windows CLI:

  - Run the **ftp** *ip-address* command to connect to the device using FTP.

    In the preceding command, *ip-address* indicates the IP address configured on the device. Routes between the terminal and the device are reachable.

 Copyright © Huawei Technologies Co., Ltd.

– Enter the user name and password as prompted and press **Enter**. If command prompt **ftp>** is displayed in the FTP client view, the user accesses the working directory on the FTP server. (The following information is only for reference.)

```
C:\Windows\System32> ftp 192.168.150.208
Connected to 192.168.150.208.
220 FTP service ready.
User(192.168.150.208:(none)):huawei
331 Password required for huawei.
Password:
230 User logged in.
ftp>
```

- **Run FTP commands to perform file-related operations.**

  After connecting to the FTP server, users can run FTP commands to perform file-related operations including performing operations on directories and files, configuring the file transfer mode, and viewing the online help about FTP commands.

  NOTE

  User rights are configured on the FTP server.

  Users can perform the following operations in any sequence.

Table 11-13 Running FTP commands to perform file-related operations

Operation	Command	Description
Change the working directory on the server.	**cd** *remote-directory*	-
Change the current working directory to its parent directory.	**cdup**	-
Display the working directory on the server.	**pwd**	-
Display or change the local working directory.	**lcd** [*local-directory*]	The **lcd** command displays the local working directory on the client, and the **pwd** command displays the working directory on the remote server.
Create a directory on the server.	**mkdir** *remote-directory*	The directory name can consist of letters and digits. The following special characters are not supported: < > ? \ :

 Copyright © Huawei Technologies Co., Ltd.

Operation	Command	Description
Delete a directory from the server.	**rmdir** *remote-directory*	-
Display information about the specified directory or file on the server.	**dir/ls** [*remote-filename* [*local-filename*]]	• The **ls** command displays only the directory or file name, and the **dir** command displays detailed directory or file information such as name, size, and date when the directory or file is created. • If no directory is specified in the command, the system searches for the file in user's authorized directories.
Delete a file from the server.	**delete** *remote-filename*	-
Upload a file.	**put** *local-filename* [*remote-filename*]	-
Download a file.	**get** *remote-filename* [*local-filename*]	-
Set the file transfer mode to ASCII.	**ascii**	Select one of them. • The default file transfer mode is ASCII. • The ASCII mode is used to transfer text files, and the binary mode is used to transfer programs, system software, and database files.
Set the file transfer mode to Binary.	**binary**	
Set the data transmission mode to passive.	**passive**	Select one of them. The default data transmission mode is active.
Set the data transmission mode to active.	**undo passive**	
View the online help about FTP commands.	**remotehelp** [*command*]	-

 Copyright © Huawei Technologies Co., Ltd.

Operation	Command	Description
Enable the verbose function.	**verbose**	After the verbose function is enabled, all FTP response messages are displayed on the FTP client.

- **(Optional) Change the login user.**

  The current user can switch to another user in the FTP client view. The new FTP connection is the same as that established by running the **ftp** command.

Operation	Command	Description
Change the current user in the FTP client view.	**user** *user-name* [*password*]	When the login user is switched to another user, the original user is disconnected from the FTP server.

- **Disconnect the FTP client from the FTP server.**

  Users can run different commands in the FTP client view to disconnect the FTP client from the FTP server.

Operation	Command	Description
Disconnect the FTP client from the FTP server and return to the user view.	**bye** or **quit**	Select one of them.
Disconnect the FTP client from the FTP server and return to the FTP client view.	**close** or **disconnect**	

----End

Verifying the Configuration

- Run the **display** [**ipv6**] **ftp-server** command to check the FTP server configuration and status.
- Run the **display ftp-users** command to view information about the FTP users who log in to the FTP server.

11.4.4 Managing Files When the Device Functions as an SFTP Server

SFTP allows a terminal to connect to the remote device using SSH and ensures the data transmission security.

 Copyright © Huawei Technologies Co., Ltd.

Pre-configuration Tasks

Before connecting to the SFTP server to manage files, complete the following tasks:

- Ensure that routes are reachable between the terminal and the device.
- Ensure that the SSH client software has been installed on the terminal.

Configuration Process

NOTICE

The SFTPv1 protocol will bring risk to device security. The SFTPv2 mode is recommended.

Table 11-14 describes the procedure for managing files when the device functions as an SFTP server.

Table 11-14 Managing files when the device functions as an SFTP server

No.	Task	Description	Remarks
1	Set SFTP server parameters	• Generate a local key pair. • Enable the SFTP server function. • Configure the following server parameters:Key exchange algorithm;Encryption algorithm;HMAC algorithm;Port number;Interval for updating the key pair;SSH authentication timeout duration;Number of SSH authentication retries;Physical interfaces on the SSH server to which clients can connect. • configure the SSH server to be compatible with earlier SSH versions.	The three steps can be performed in any sequence.

 Copyright © Huawei Technologies Co., Ltd.

No.	Task	Description	Remarks
2	**Configuring the VTY user interface for SSH users to log in to the device**	Configure the user authentication mode, SSH, and other basic attributes on the VTY user interface.	
3	**Configure SSH user information**	Create an SSH user and set the authentication mode on the SFTP server.	
4	**Connect to the device using SFTP**	Connect to the device using the SSH client software on the terminal.	-

Default Parameter Settings

Table 11-15 Default parameter settings

Parameter	Default Value
SFTP server function	Disabled.
Key exchange algorithm	Earlier versions of V200R010C10: All key exchange algorithms. V200R010C10 and later versions: **dh_group_exchange_sha1** and **dh_group14_sha1**.
Encryption algorithm	Earlier versions of V200R010C10: Encryption algorithms except DES-CBC are in the encryption algorithm list of an SSH server. V200R010C10 and later versions: **aes128_ctr**, **aes192_ctr**, and **aes256_ctr**.
HMAC algorithm	Earlier versions of V200R010C10: All HMAC algorithms. V200R010C10 and later versions: **sha2_256**.
Listening port number	22.
Time for updating the key pair of the server	0, indicating the key pair of the server is never updated.
SSH authentication timeout duration	60 seconds.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Default Value
Number of SSH authentication retries	3.
SSH user	No SSH user is created.

Procedure

- **Set SFTP server parameters.**

  Table 11-16 Setting SFTP server parameters

Operation	Command	Description
Enter the system view.	**system-view**	-
Generate the local RSA or ECC key pair.	**rsa local-key-pair create** or **ecc local-key-pair create**	Run the **display rsa local-key-pair public** or **display ecc local-key-pair public** command to view the public key in the local RSA key pair. Configure the public key on the SSH server. **NOTE** Because a longer key pair provides higher security, you are advised to use key pairs of the largest length.
Enable the SFTP server function.	**sftp server enable**	By default, the SFTP server function is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Operation	Command	Description
(Optional) Configure a key exchange algorithm list for the SSH server.	**ssh server key-exchange** { **dh_group_exchange_sha1** | **dh_group14_sha1** | **dh_group1_sha1** } *	Earlier versions of V200R010C10: By default, an SSH server supports all key exchange algorithms. V200R010C10 and later versions: By default, an SSH server supports the following key exchange algorithms: **dh_group_exchange_sha1** and **dh_group14_sha1**. During the negotiation process, the client and server negotiate the key exchange algorithm for packet transmission. You can perform this step to configure a key exchange algorithm list for the SSH server. The server compares the key exchange algorithm list sent by the client with its own key exchange algorithm list, and selects the first key exchange algorithm on the client's list that matches a key exchange algorithm on its own list as the key exchange algorithm for packet transmission. If no algorithm on the client's list matches an algorithm on the server's list, the negotiation fails.

 Copyright © Huawei Technologies Co., Ltd.

Operation	Command	Description
(Optional) Configure an encryption algorithm list for the SSH server.	**ssh server cipher**{ **3des_cbc** | **aes128_cbc** | **aes128_ctr** | **aes192_ctr** | **aes256_ctr** | **blowfish_cbc** | **des_cbc** } *	Earlier versions of V200R010C10: By default, encryption algorithms except DES-CBC are in the encryption algorithm list of an SSH server. V200R010C10 and later versions: By default, an SSH server supports the following encryption algorithms: **aes128_ctr**, **aes192_ctr**, and **aes256_ctr**. During the negotiation process, the client and server negotiate the encryption algorithm for packet transmission. You can perform this step to configure an encryption algorithm list for the SSH server. The server compares the encryption algorithm list sent by the client with its own encryption algorithm list, and selects the first encryption algorithm on the client's list that matches an encryption algorithm on its own list as the encryption algorithm for packet transmission. If no algorithm on the client's list matches an algorithm on the server's list, the negotiation fails.

 Copyright © Huawei Technologies Co., Ltd.

Operation	Command	Description
(Optional) Configure an HMAC algorithm list for the SSH server.	**ssh server hmac** { **md5** | **md5_96** | **sha1** | **sha1_96** | **sha2_256** | **sha2_256_96** } *	Earlier versions of V200R010C10: By default, an SSH server supports all HMAC algorithms. V200R010C10 and later versions: By default, an SSH server supports the **sha2_256** encryption algorithms only. During the negotiation process, the client and server negotiate the HMAC algorithm for packet transmission. You can perform this step to configure an HMAC algorithm list for the SSH server. The server compares the HMAC algorithm list sent by the client with its own HMAC algorithm list, and selects the first HMAC algorithm on the client's list that matches an HMAC algorithm on its own list as the HMAC algorithm for packet transmission. If no algorithm on the client's list matches an algorithm on the server's list, the negotiation fails.
(Optional) Configure the listening port number.	**ssh server port** *port-number*	By default, the listening port number is 22. If a new port number is configured, the SSH server disconnects from all SSH clients and uses the new port number to listen to connection requests. Attackers do not know the port number and cannot access the listening port of the SSH server.

 Copyright © Huawei Technologies Co., Ltd.

Operation	Command	Description
(Optional) Configure the interval for updating the key pair of the server.	**ssh server rekey-interval** *hours*	By default, the interval for updating the key pair is 0. The value **0** indicates that the key pair is never updated. After the interval for updating the SSH server key pair is set using this command, the system will automatically update the key pair at intervals, which ensures security.
(Optional) Configure the SSH authentication timeout duration.	**ssh server timeout** *seconds*	By default, the SSH authentication timeout duration is 60 seconds.
(Optional) Configure the number of SSH authentication retries.	**ssh server authentication-retries** *times*	By default, the number of SSH authentication retries is 3.
(Optional) Enable earlier versions to be compatible.	**ssh server compatible-ssh1x enable**	By default, the server's compatibility with earlier versions is disabled.
(Optional) Specify physical interfaces on the SSH server to which clients can connect.	**ssh server permit interface** { *interface-type interface-number* } &<1-5>	By default, clients can connect to all the physical interfaces on the SSH server.

  - When the local RSA or ECC key pair is generated, two key pairs (a server key pair and a host key pair) are generated at the same time. Each key pair contains a public key and a private key. The length of the two key pairs ranges from 512 bits to 2048 bits. The default length is 2048 bits.

- **Configure the VTY user interface for SSH users to log in to the device.**

  SSH users use the VTY user interface to log in to the device using SFTP. Attributes of the VTY user interface must be configured.

  Table 11-17 Configuring the VTY user interface for SSH users to log in to the device

Operation	Command	Description
Enter the system view.	**system-view**	-

 Copyright © Huawei Technologies Co., Ltd.

Operation	Command	Description
Enter the VTY user interface view.	**user-interface vty** *first-ui-number* [*last-ui-number*]	-
Set the authentication mode of the VTY user interface to **AAA**.	**authentication-mode aaa**	By default, no authentication mode is configured for the VTY user interface. The authentication mode of the VTY user interface must be set to **AAA**. Otherwise, you cannot configure the **protocol inbound ssh** command and users cannot log in to the device.
Configure a VTY user interface that supports SSH.	**protocol inbound ssh**	By default, the VTY user interface supports SSH. If no VTY user interface supports SSH, users cannot log in to the device.
Configure the user level.	**user privilege level** *level*	The user level must be set to **3** or higher to ensure successful connection establishment. If a local user uses password authentication, you can run the **local-user** *user-name* **privilege level** *level* command to set the level of the user to 3 or higher.
(Optional) Configure other attributes of the VTY user interface.	-	Other attributes of the VTY user interface are as follows: • Maximum number of VTY user interfaces • Restrictions on incoming calls and outgoing calls on the VTY user interface • Terminal attributes on the VTY user interface For details, see **9.6.1 (Optional) Configuring Attributes for a VTY User Interface**.

- **Configure SSH user information.**

 Copyright © Huawei Technologies Co., Ltd.

Configure SSH user information including the authentication mode. Authentication modes including RSA, ECC, password, password-rsa, password-ecc, and all are supported.

- The password-rsa authentication mode consists of the password and RSA authentication modes.
- The password-ecc authentication mode consists of the password and ECC authentication modes.
- The all authentication mode indicates that SSH users only need to authenticated by ECC, password, or RSA.
- If the SSH user uses the password authentication mode, only the SSH server needs to generate the RSA, or ECC key. If the SSH user uses the RSA authentication mode, both the SSH server and client need to generate the RSA, or ECC key and configure the public key of the peer end locally.

Table 11-18 Configuring SSH user information

Operation	Command	Description
Enter the system view.	**system-view**	-
Enter the AAA view.	**aaa**	-
Create SSH users.	**local-user** *user-name* **password irreversible-cipher** *password*	-
Configure the SSH user level.	**local-user** *user-name* **privilege level** *level*	The local user level must be set to **3** or higher. This operation cannot be performed if the user level in the VTY interface view has been set to 3 or higher using the **user privilege level** *level* command.
Configure the service type for SSH users.	**local-user** *user-name* **service-type ssh**	-
Configure the authorized directory for SSH users.	**local-user** *user-name* **ftp-directory** *directory*	By default, the authorized directory for an SSH user is the root directory of the default storage medium.

 Copyright © Huawei Technologies Co., Ltd.

Operation		Command	Description
Return to the system view.		**quit**	-
Configure the authentication mode for SSH users.		**ssh user** *user-name* **authentication-type** { **password** | **rsa** | **ecc** | **password-rsa** | **password-ecc** | **all** }	-
If any one of the following authentication modes is configured for SSH users: • rsa • ecc • password-rsa • password-ecc	Enter the RSA or ECC public key view.	**rsa peer-public-key** *key-name* [**encoding-type** { **der** | **openssh** | **pem** }] or **ecc peer-public-key** *key-name* **encoding-type** { **der** | **openssh** | **pem** }	-
	Enter the public key editing view.	**public-key-code begin**	-
	Edit the public key.	*hex-data*	• The public key must be a hexadecimal character string in the public key format generated by the SSH client software. For details, see SSH client software help. • Copy and paste the RSA public key to the device that functions as the SSH server.
	Exit the public key editing view.	**public-key-code end**	-
	Return to the system view.	**peer-public-key end**	-
	Assign an RSA or ECC public key to an SSH user.	**ssh user** *user-name* **assign rsa-key** | **ecc-key** } *key-name*	-

 Copyright © Huawei Technologies Co., Ltd.

- **Connect to the device using SFTP.**

  The SSH client software supporting SFTP must be installed on the terminal to ensure that the terminal can connect to the device using SFTP to manage files. The following describes how to connect to the device using the OpenSSH and the Windows CLI.

  - For details how to install the OpenSSH, see the OpenSSH installation description.
  - To use the OpenSSH to connect to the device using SFTP, run the OpenSSH commands. For details about OpenSSH commands, see OpenSSH help.
  - Windows command prompt can identify commands supported by the OpenSSH only when the OpenSSH is installed on the terminal.

  Access the Windows CLI and run the commands supported by the OpenSSH to connect to the device using SFTP to manage files.

  If command prompt **sftp>** is displayed in the SFTP client view, the user accesses the working directory on the SFTP server. (The following information is only for reference.)

```
C:\Documents and Settings\Administrator> sftp client001@192.168.200.161
Connecting to 192.168.200.161...
The authenticity of host '192.168.200.161 (192.168.200.161)' can't be established.
RSA key fingerprint is 46:b2:8a:52:88:42:41:d4:af:8f:4a:41:d9:b8:4f:ee.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.200.161' (RSA) to the list of known hosts.

client001@192.168.200.161's password:
sftp>
```

- **Run SFTP commands to perform file-related operations.**

  In the SFTP client view, you can perform one or more file-related operations listed in **Table 11-19** in any sequence.

  NOTE

  In the SFTP client view, the system does not support predictive command input. Therefore, you must enter commands in full name.

Table 11-19 Running SFTP commands to perform file-related operations

Operation	Command	Description
Change the user's current working directory.	**cd** [*remote-directory*]	-
Change the current working directory to its parent directory.	**cdup**	-
Display the user's current working directory.	**pwd**	-

 Copyright © Huawei Technologies Co., Ltd.

Operation	Command	Description
Display the file list in a specified directory.	**dir/ls** [**-l** | **-a**] [*remote-directory*]	Outputs of the **dir** and **ls** commands are the same.
Delete directories from the server.	**rmdir** *remote-directory* &<1-10>	A maximum of 10 directories can be deleted at one time. Before running the **rmdir** command to delete directories, ensure that the directories do not contain any files. Otherwise, the deletion fails.
Create a directory on the server.	**mkdir** *remote-directory*	-
Change the name of a specified file on the server.	**rename** *old-name new-name*	-
Download a file from the remote server.	**get** *remote-filename* [*local-filename*]	-
Upload a local file to the remote server.	**put** *local-filename* [*remote-filename*]	-
Delete files from the server.	**remove** *remote-filename* &<1-10>	A maximum of 10 files can be deleted at one time.
View the help about SFTP commands.	**help** [**all** | *command-name*]	-

- **Disconnect the SFTP client from the SSH server.**

Operation	Command	Description
Disconnect the SFTP client from the SSH server.	**quit**	-

----End

Verifying the Configuration

- Run the **display ssh user-information** [*username*] command to view SSH user information on the SSH server.

 Copyright © Huawei Technologies Co., Ltd.

- Run the **display ssh server status** command to view global configuration of the SSH server.
- Run the **display ssh server session** command to view session information of the SSH client on the SSH server.

11.5 File Management on Other Devices

11.5.1 Managing Files When the Device Functions as a TFTP Client

The device can function as a TFTP client to log in to the TFTP server remotely to upload or download files.

Pre-configuration Tasks

Before connecting to a device as a TFTP client to manage files, complete the following tasks:

- Ensure that routes are reachable between the current device and the TFTP server.
- Obtain the host name or IP address of the TFTP server and the directory for storing files to be downloaded or uploaded.

Configuration Process

NOTE

The TFTP protocol will bring risk to device security. The SFTPv2 mode is recommended.

Table 11-20 describes the procedure for managing files when the device functions as a TFTP client.

Table 11-20 Procedure for managing files when the device functions as a TFTP client

No.	Task	Description	Remarks
1	**(Optional) Configure the TFTP client source address**	Configure the TFTP client source address. To ensure communication security, the source address can be set to a source IP address or source interface.	You can configure the TFTP client source address and TFTP ACL rule in any sequence.
2	**(Optional) Configure the TFTP ACL**	Configure the ACL rule and TFTP basic ACL to improve TFTP access security.	You can configure the TFTP client source address and TFTP ACL rule in any sequence.

 Copyright © Huawei Technologies Co., Ltd.

No.	Task	Description	Remarks
3	**Run TFTP commands to upload or download files**	Upload and download files.	You can configure the TFTP client source address and TFTP ACL rule in any sequence.

Procedure

- **(Optional) Configure the TFTP client source address.**

  When you specify the source address in an ACL, use the address of an interface in stable state, for example, a loopback interface. This simplifies the ACL rule and security policy configuration. After the client source address is configured as the source or destination address in the ACL rule, IP address differences and interface status impact are shielded, and incoming and outgoing packets are filtered.

  Table 11-21 (Optional) Configuring the TFTP client source address

Operation	Command	Description
Enter the system view.	**system-view**	-
Configure the TFTP client source address.	**tftp client-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* }	The TFTP client source address can be set to a source IP address or source interface. If the source address is set to source interface, configure an IP address for the interface for establishing TFTP connections.

- **(Optional) Configure the TFTP ACL.**

  An ACL is composed of a list of rules such as the source address, destination address, and port number of packets. ACL rules are used to classify packets. After these rules are applied to routing devices, the routing devices determine the packets to be received and rejected.

  An ACL can define multiple rules. ACLs are classified into basic ACLs, advanced ACLs, and Layer 2 ACLs.

  TFTP supports only the basic ACL whose number ranges from 2000 to 2999.

  ACL rule:

 Copyright © Huawei Technologies Co., Ltd.

– If **permit** is defined in an ACL rule, the device can establish TFTP connections with any devices that match the rule.
– If **deny** is defined in an ACL rule, the device cannot establish TFTP connections with devices that match the rule.

Table 11-22 (Optional) Configuring the TFTP ACL

Operation	Command	Description
Enter the system view.	**system-view**	-
Create an ACL and enter the ACL view.	**acl** [**number**] *acl-number*	By default, no ACL is created.
Configure the ACL rule.	**rule** [*rule-id*] { **deny** | **permit** } [**source** { *source-address source-wildcard* | **any** } | **vpn-instance** *vpn-instance-name* | [**fragment** | **none-first-fragment**] | **logging** | **time-range** *time-name*] *	By default, no ACL rule is configured.
Return to the system view.	**quit**	-
Configure the TFTP ACL.	**tftp-server acl** *acl-number*	-

- **Run TFTP commands to upload or download files.**

Operation	Command	Description
IPv4 address	**tftp** [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *tftp-server* [**public-net** | **vpn-instance** *vpn-instance-name*] { **get** | **put** } *source-filename* [*destination-filename*]	Run either of the commands based on the IP address type. • **get**: downloads a file. • **put**: uploads a file.
IPv6 address	**tftp ipv6** [**-a** *source-ip-address*] *tftp-server-ipv6* [**-oi** *interface-type interface-number*] [**vpn6-instance** *vpn6-instance-name*] { **get** | **put** } *source-filename* [*destination-filename*]	

 Copyright © Huawei Technologies Co., Ltd.

NOTE

You can use either or both of the following methods to increase the TFTP uploading or downloading rate.

- Use the third-party software TFTPD32 (Windows operating system) or TFTPD-HPA (Linux operating system) on the TFTP server.
- Configure CPCAR on the TFTP client to increase the rate threshold. After performing the TFTP operation, run the **undo cpu-defend-policy** [**global** | **slot** *slot-id*] command to cancel the application of an attack defense policy.

The source address or interface specified in the **tftp** command has a higher priority than that specified in the **tftp client-source** command. If you specify different source addresses or interfaces in the **tftp client-source** and **tftp** commands, the source address or interface specified in the **tftp** command takes effect. The source address or interface specified in the **tftp client-source** command applies to all TFTP connections. The source address or interface specified in the **tftp** command applies only to the current TFTP connection.

----End

Verifying the Configuration

- Run the **display tftp-client** command to check source address of the TFTP client.
- Run the **display acl** { *acl-number* | **all** } command to check the ACL configurations of the TFTP client.

11.5.2 Managing Files When the Device Functions as an FTP Client

The device functions as an FTP client and connects to an FTP server remotely to transfer files and manage files and directories on the FTP server.

Pre-configuration Tasks

Before connecting to a device as an FTP client to manage files, complete the following tasks:

- Ensure that routes are reachable between the current device and the FTP server.
- Obtain the host name or IP address of the FTP server, FTP user name, and password.
- Obtain the listening port number of the FTP server if the default listening port number is not used.

Configuration Process

NOTICE

The FTP protocol will bring risk to device security. The SFTPv2 mode is recommended.

 Copyright © Huawei Technologies Co., Ltd.

Table 11-23 describes the procedure for managing files when the device functions as an FTP client.

Table 11-23 Procedure for managing files when the device functions as an FTP client

No.	Task	Description	Remarks
1	**(Optional) Configure the FTP client source address**	Configure the FTP client source address. To ensure communication security, the source address can be set to a source IP address or source interface.	Perform steps 1 and 2 in sequence. After the FTP connection is established, perform steps 3 and 4 in any sequence. To disconnect from the FTP server, perform step 5.
2	**Run FTP commands to connect to the FTP server**	-	
3	**Run FTP commands to perform file-related operations**	Run FTP commands to perform file-related operations including performing operations on directories and files, configuring the file transfer mode, and viewing the online help about FTP commands.	
4	**(Optional) Change the login user**	-	
5	**Disconnect the FTP client from the FTP server**	-	

Procedure

- **(Optional) Configure the FTP client source address.**

  When you specify the source address in an ACL, use the address of an interface in stable state, for example, a loopback interface. This simplifies the ACL rule and security policy configuration. After the client source address is configured as the source or destination address in the ACL rule, IP address differences and interface status impact are shielded, and incoming and outgoing packets are filtered.

  The FTP client source address must be set to the loopback interface IP address or loopback interface.

 Copyright © Huawei Technologies Co., Ltd.

Table 11-24 Configuring the FTP client source address

Operation	Command	Description
Enter the system view.	**system-view**	-
Configure the FTP client source address.	**ftp client-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* }	You are advised to use the loopback interface IP address. When the FTP client source address is set to loopback interface, configure an IP address for the loopback interface for establishing FTP connections.

- **Run FTP commands to connect to the FTP server.**

  Run the corresponding command in the user view or FTP client view to connect to the FTP server.

  Perform the following operations based on the server IP address types.

  Table 11-25 Running FTP commands to connect to the FTP server (with an IPv4 address)

Operation	Command	Description
Connect to the FTP server in the user view when the server uses an IPv4 address.	**ftp** [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *host-ip* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]	Select one of them. To enter the FTP client view, run the **ftp** command.
Connect to the FTP server in the FTP client view when the server uses an IPv4 address.	**ftp**	
	open [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *host-ip* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]	

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- Before connecting to the FTP server, run the **set net-manager vpn-instance** command to set the VPN instance to the default VPN instance.
- The source address specified in the **ftp** command has a higher priority than that specified in the **ftp client-source** command on an IPv4 network. If you specify different source addresses in the **ftp client-source** and **ftp** commands, the source address specified in the **ftp** command takes effect. The source address specified in the **ftp client-source** command applies to all TFTP connections. The source address specified in the **ftp** command applies only to the current TFTP connection.

Table 11-26 Running FTP commands to connect to the FTP server (with an IPv6 address)

Operation	Command	Description
Connect to the FTP server in the user view when the server uses an IPv6 address.	**ftp ipv6** *host-ipv6* [**vpn6-instance** *vpn6-instance-name*] [*port-number*]	Select one of them. To enter the FTP client view, run the **ftp** command.
Connect to the FTP server in the FTP client view when the server uses an IPv6 address.	**ftp**	
	open ipv6 *host-ipv6* [*port-number*]	

Users must enter the correct user name and password to connect to the server.

- **Run FTP commands to perform file-related operations.**

  After connecting to the FTP server, users can run FTP commands to perform file-related operations including performing operations on directories and files, configuring the file transfer mode, and viewing the online help about FTP commands.

  NOTE

  User rights are configured on the FTP server.

  Users can perform the following operations in any sequence.

Table 11-27 Running FTP commands to perform file-related operations

Operation	Command	Description
Change the working directory on the server.	**cd** *remote-directory*	-

Operation	Command	Description
Change the current working directory to its parent directory.	**cdup**	-
Display the working directory on the server.	**pwd**	-
Display or change the local working directory.	**lcd** [*local-directory*]	The **lcd** command displays the local working directory on the client, and the **pwd** command displays the working directory on the remote server.
Create a directory on the server.	**mkdir** *remote-directory*	The directory name can consist of letters and digits. The following special characters are not supported: < > ? \ :
Delete a directory from the server.	**rmdir** *remote-directory*	-
Display information about the specified directory or file on the server.	**dir/ls** [*remote-filename* [*local-filename*]]	• The **ls** command displays only the directory or file name, and the **dir** command displays detailed directory or file information such as name, size, and date when the directory or file is created. • If no directory is specified in the command, the system searches for the file in user's authorized directories.
Delete a file from the server.	**delete** *remote-filename*	-
Upload a file.	**put** *local-filename* [*remote-filename*]	-
Download a file.	**get** *remote-filename* [*local-filename*]	-
Set the file transfer mode to ASCII.	**ascii**	Select one of them. • The default file transfer mode is ASCII.

 Copyright © Huawei Technologies Co., Ltd.

Operation	Command	Description
Set the file transfer mode to Binary.	**binary**	• The ASCII mode is used to transfer text files, and the binary mode is used to transfer programs, system software, and database files.
Set the data transmission mode to passive.	**passive**	Select one of them. The default data transmission mode is active.
Set the data transmission mode to active.	**undo passive**	
View the online help about FTP commands.	**remotehelp** [*command*]	-
Enable the verbose function.	**verbose**	After the verbose function is enabled, all FTP response messages are displayed on the FTP client.

- **(Optional) Change the login user.**

  The current user can switch to another user in the FTP client view. The new FTP connection is the same as that established by running the **ftp** command.

Operation	Command	Description
Change the current user in the FTP client view.	**user** *user-name* [*password*]	When the login user is switched to another user, the original user is disconnected from the FTP server.

- **Disconnect the FTP client from the FTP server.**

  Users can run different commands in the FTP client view to disconnect the FTP client from the FTP server.

Operation	Command	Description
Disconnect the FTP client from the FTP server and return to the user view.	**bye** or **quit**	Select one of them.

 Copyright © Huawei Technologies Co., Ltd.

Operation	Command	Description
Disconnect the FTP client from the FTP server and return to the FTP client view.	**close** or **disconnect**	

----End

Verifying the Configuration

- Run the **display ftp-client** command to check source interface of the FTP client.

11.5.3 Managing Files When the Device Functions as an SFTP Client

SFTP is an SSH-based protocol that provides a secure file transfer capability. After you configure the device as an SFTP client, the remote SSH server authenticates the SFTP client and encrypts data in bidirectional mode. This ensures secure file transfer and management of directories on the SSH server.

Pre-configuration Tasks

Before connecting to a device as an SFTP client to manage files, complete the following tasks:

- Ensure that routes are reachable between the current device and the SSH server.
- Obtain the host name or IP address of the SSH server and SSH user information.
- Obtain the listening port number of the SSH server if the default listening port number is not used.

NOTICE

Because a longer key pair provides higher security, you are advised to use key pairs of the largest length.

Configuration Process

Table 11-28 describes the procedure for managing files when the device functions as an SFTP client.

 Copyright © Huawei Technologies Co., Ltd.

Table 11-28 Procedure for managing files when the device functions as an SFTP client

No.	Task	Description	Remarks
1	**(Optional) Configure the SFTP client source address**	Configure the SFTP client source address. To ensure communication security, the source address can be set to a source IP address or source interface.	Steps 1, 2, and 3 can be performed in any sequence. Steps 4-6 need to be performed in sequence.
2	**Generate a local key pair**	Generate a local key pair and configure the public key on the SSH server. Perform this step only when the device logs in to the SSH server in RSA or ECC authentication mode, not the password authentication mode.	
3	**Configure the initial SSH connection**	To configure the initial SSH connection, enable the initial authentication function or save the public key of the SSH server on the SSH client.	
4	**Run SFTP commands to connect to the SSH server**	-	
5	**Run SFTP commands to perform file-related operations**	Users can perform operations on directories and files on the SSH server and view the help about SFTP commands on the SFTP client.	
6	**Disconnect the SFTP client from the SSH server**	-	

Procedure

- **(Optional) Configure the SFTP client source address.**

  When you specify the source address in an ACL, use the address of an interface in stable state, for example, a loopback interface. This simplifies the ACL rule and security policy configuration. After the client source address is configured as the source or destination address in the ACL rule, IP address differences and interface status impact are shielded, and incoming and outgoing packets are filtered.

  The SFTP client source address must be set to the loopback interface IP address or loopback interface.

 Copyright © Huawei Technologies Co., Ltd.

Table 11-29 Configuring the SFTP client source address

Operation	Command	Description
Enter the system view.	**system-view**	-
Configure the SFTP client source address.	**sftp client-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* }	The default source address is 0.0.0.0.

- **Generate a local key pair.**

  NOTE

  Perform this step only when the device logs in to the SSH server in RSA, or ECC authentication mode, not the password authentication mode.

  Table 11-30 Actions for generating a local key pair

Action	Command	Description
Enter the system view.	**system-view**	-
Generate the local RSA or ECC key pair.	**rsa local-key-pair create** or **ecc local-key-pair create**	Run the **display rsa local-key-pair public** or **display ecc local-key-pair public** command to view the public key in the local RSA or ECC key pair. Configure the public key on the SSH server. **NOTE** Because a longer key pair provides higher security, you are advised to use key pairs of the largest length.

- **Configure the initial SSH connection.**

  By default, the client cannot connect to the SSH server because the client does not save the public key of the SSH server. Configure the initial SSH connection in either of the following ways:

  - Enable the initial authentication function on the client. With the function enabled, the client connects to the SSH server without checking the public key of the SSH server. When the initial SSH connection succeeds, the client automatically saves the public key of the SSH server for the next SSH connection. For details, see **Table 11-31**.
  - Save the public key of the SSH server on the client so that the client can authenticate the SSH server successfully. For details, see **Table 11-32**. This method ensures higher security but becomes more complex than the first method.

 Copyright © Huawei Technologies Co., Ltd.

Table 11-31 Actions for enabling first authentication for the SSH client

Action	Command	Description
Enter the system view.	**system-view**	-
Enable first authentication for the SSH client.	**ssh client first-time enable**	By default, first authentication is disabled on the SSH client.

Table 11-32 Actions for configuring the SSH client to assign the RSA or ECC public key to the SSH server

Action	Command	Description
Enter the system view.	**system-view**	-
Enter the RSA or ECC public key view.	**rsa peer-public-key** *key-name* or **ecc peer-public-key** *key-name*	-
Enter the public key editing view.	**public-key-code begin**	-
Edit the public key.	*hex-data*	• The public key must be a hexadecimal character string in the public key encoding format, and generated by the SSH server. • After entering the public key editing view, you must enter the RSA or ECC public key that is generated on the server to the client.

 Copyright © Huawei Technologies Co., Ltd.

Action	Command	Description
Quit the public key editing view.	**public-key-code end**	• If no key public code hex-data is entered, the public key cannot be generated after you run this command. • If the specified key *keyname* has been deleted, the system displays a message indicating that the key does not exist and returns to the system view directly when you run this command.
Return to the system view.	**peer-public-key end**	-
Bind the RSA or ECC public key to the SSH server.	**ssh client** *servername* **assign**{ **rsa-key** | **ecc-key** } *keyname*	If the SSH server public key saved in the SSH client does not take effect, run the **undo ssh client** *servername* **assign**{ **rsa-key** | **ecc-key** } command to cancel the binding between the SSH server and RSA or ECC public key, and run this command to assign a new RSA, or ECC public key to the SSH server.

- **Run SFTP commands to connect to the SSH server.**

  The command for connecting an SFTP client is similar to that for connecting the STelnet client. Both the clients can carry the source address, support the keepalive function, and select a key exchange algorithm, an encryption algorithm, and an HMAC algorithm.

  Table 11-33 Running SFTP commands to connect to the SSH server

Operation	Command	Description
Enter the system view.	**system-view**	-

 Copyright © Huawei Technologies Co., Ltd.

Operation	Command	Description
IPv4 address	**sftp** [**-a** *source-address* | **-i** *interface-type interface-number*] *host-ip* [*port*] [[**public-net** | **-vpn-instance** *vpn-instance-name*] | [**prefer_kex** { **dh_group1** | **dh_exchange_group** }] | [**prefer_ctos_cipher** { **des** | **3des** | **aes128** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** }] | [**prefer_stoc_cipher** { **des** | **3des** | **aes128** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** }] | [**prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] | [**prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }]] * [**-ki** *aliveinterval* [**-kc** *alivecountmax*]]	Run either of the commands based on the IP address type. In most cases, only the IP address is specified in the commands. **NOTE** DES, 3DES, MD5, MD5_96, SHA1, and SHA1_96 encryption algorithm cannot ensure security. AES128, AES128-CTR, AES192-CTR or AES256-CTR encryption algorithm is recommended.
IPv6 address	**sftp ipv6** [**-a** *source-address*] *host-ipv6* [**-oi** *interface-type interface-number*] [*port*] [[**-vpn6-instance** *vpn-instance-name*] | [**prefer_kex** { **dh_group1** | **dh_exchange_group** }] | [**prefer_ctos_cipher** { **des** | **3des** | **aes128** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** }] | [**prefer_stoc_cipher** { **des** | **3des** | **aes128** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** }] | [**prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] | [**prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }]] * [**-ki** *aliveinterval* [**-kc** *alivecountmax*]]	

Command example:

```
[Huawei] sftp 10.137.217.201
```

When the SSH connection succeeds, **sftp-client>** is displayed, indicating the SFTP client view is displayed.

- **Run SFTP commands to perform file-related operations.**

  In the SFTP client view, you can perform one or more file-related operations listed in **Table 11-34** in any sequence.

  NOTE

  In the SFTP client view, the system does not support predictive command input. Therefore, you must enter commands in full name.

 Copyright © Huawei Technologies Co., Ltd.

Table 11-34 Running SFTP commands to perform file-related operations

Operation	Command	Description
Change the user's current working directory.	**cd** [*remote-directory*]	-
Change the current working directory to its parent directory.	**cdup**	-
Display the user's current working directory.	**pwd**	-
Display the file list in a specified directory.	**dir/ls** [**-l** | **-a**] [*remote-directory*]	Outputs of the **dir** and **ls** commands are the same.
Delete directories from the server.	**rmdir** *remote-directory* &<1-10>	A maximum of 10 directories can be deleted at one time. Before running the **rmdir** command to delete directories, ensure that the directories do not contain any files. Otherwise, the deletion fails.
Create a directory on the server.	**mkdir** *remote-directory*	-
Change the name of a specified file on the server.	**rename** *old-name new-name*	-
Download a file from the remote server.	**get** *remote-filename* [*local-filename*]	-
Upload a local file to the remote server.	**put** *local-filename* [*remote-filename*]	-
Delete files from the server.	**remove** *remote-filename* &<1-10>	A maximum of 10 files can be deleted at one time.
View the help about SFTP commands.	**help** [**all** | *command-name*]	-

- **Disconnect the SFTP client from the SSH server.**

 Copyright © Huawei Technologies Co., Ltd.

Operation	Command	Description
Disconnect the SFTP client from the SSH server.	**quit**	-

----End

Verifying the Configuration

- Run the **display sftp-client** command to check source interface of the SFTP client.

11.6 Configuration Examples for File Management

11.6.1 Example of Logging In to the Device to Manage Files

Networking Requirements

After logging in to the device through the console interface, Telnet, or STelnet, perform the following operations:

- View files and subdirectories in the current directory.
- Create the **test** directory, copy the **vrpcfg.zip** file to **test**, and rename **vrpcfg.zip** as **backup.zip**.
- View files in the **test** directory.

Procedure

Step 1 View files and subdirectories in the current directory.

```
<Huawei> system-view
[Huawei] sysname Switch
[Switch] quit
<Switch> dir
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time(LMT)  FileName
    0  -rw-           889  Mar 01 2012 14:41:56   private-data.txt
    1  -rw-         6,311  Feb 17 2012 14:05:04   backup.cfg
    2  -rw-         2,393  Mar 06 2012 17:20:10   vrpcfg.zip
    3  -rw-           812  Dec 12 2011 15:43:10   hostkey
    4  drw-             -  Mar 01 2012 14:41:46   compatible
    5  -rw-           540  Dec 12 2011 15:43:12   serverkey
...
1,927,220 KB total (1,130,464 KB free)
```

Step 2 Create the **test** directory, copy the **vrpcfg.zip** file to **test**, and rename **vrpcfg.zip** as **backup.zip**.

Create the **test** directory.

```
<Switch> mkdir test
Info: Create directory flash:/test.....Done.
```

Copy the **vrpcfg.zip** file to **test** and rename **vrpcfg.zip** as **backup.zip**.

```
<Switch> copy vrpcfg.zip flash:/test/backup.zip
Copy flash:/vrpcfg.zip to flash:/test/backup.zip?[Y/N]:y
100%  complete
Info: Copied file flash:/vrpcfg.zip to flash:/test/backup.zip...Done.
```

NOTE

If no target file name is specified, the source file and target file have the same name.

Step 3 View files in the **test** directory.

Access the **test** directory.

```
<Switch> cd test
```

View the current working directory.

```
<Switch> pwd
flash:/test
```

View files in the **test** directory.

```
<Switch> dir
Directory of flash:/test/

  Idx  Attr     Size(Byte)  Date       Time(LMT)  FileName
    0  -rw-         2,399  Mar 12 2012 11:16:44   backup.zip

1,927,220 KB total (1,130,460 KB free)
```

----End

Configuration File

Configuration file of the Switch

```
#
sysname Switch
#
return
```

11.6.2 Example for Managing Files When the Device Functions as a TFTP Server

Networking Requirements

As shown in **Figure 11-1**, there are reachable routes between the TFTP server and client. You need to obtain system software from the TFTP server to upgrade the TFTP client.

Figure 11-1 Networking diagram for managing files using TFTP



 Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the TFTP server function and related parameters.
2. Set up a connection between the TFTP server and client, and download system software from the TFTP server to the TFTP client.

Procedure

Step 1 Configure the TFTP server function and parameters.

```
<Huawei> system-view
[Huawei] sysname TFTP Server
[TFTP Server] set default tftp-directory flash:
[TFTP Server] tftp server enable
[TFTP Server] quit
```

Step 2 Set up a connection between the TFTP server and client, and download system software from the TFTP server to the TFTP client.

```
<Huawei> system-view
[Huawei] sysname TFTP Client
[TFTP Client] quit
<TFTP Client> tftp 10.1.1.1 get devicesoft.cc
Info: Transfer file in binary mode.
Downloading the file from the remote TFTP server. Please wait...

93832832 bytes received in 722 second.
TFTP: Downloading the file successfully.
```

Step 3 Verify the configuration.

Run the **dir** command on the TFTP client to check whether system software is downloaded to the TFTP client.

```
<TFTP Client> dir
Directory of flash:/

 Idx  Attr     Size(Byte)  Date       Time(LMT)  FileName
   0  -rw-           14  Mar 13 2012 14:13:38   back_time_a
   1  drw-            -  Mar 11 2012 00:58:54   logfile
   2  -rw-            4  Nov 17 2011 09:33:58   snmpnotilog.txt
   3  -rw-       11,238  Mar 12 2012 21:15:56   private-data.txt
   4  -rw-        7,717  Mar 12 2012 21:15:54   vrpcfg.zip
   5  -rw-           14  Mar 13 2012 14:13:38   back_time_b
   6  -rw-   93,832,832  Mar 13 2012 14:24:24   devicesoft.cc
   7  drw-            -  Oct 31 2011 10:20:28   sysdrv
   8  drw-            -  Feb 21 2012 17:16:36   compatible
   9  drw-            -  Feb 09 2012 14:20:10   selftest
  10  -rw-       19,174  Feb 20 2012 18:55:32   backup.cfg
  11  -rw-       43,496  Dec 15 2011 20:59:36   20111215.zip
  12  -rw-          588  Nov 04 2011 13:54:04   servercert.der
  13  -rw-          320  Nov 04 2011 13:54:26   serverkey.der
  14  drw-            -  Nov 04 2011 13:58:36   security

468,560 KB total (197,728 KB free)
```

----End

Configuration Files

- Configuration file of the TFTP server

```
#
 sysname TFTP Server
#
```

 Copyright © Huawei Technologies Co., Ltd.

```
 set default tftp-directory flash:
 tftp server enable
#
return
```

- Configuration file of the TFTP client

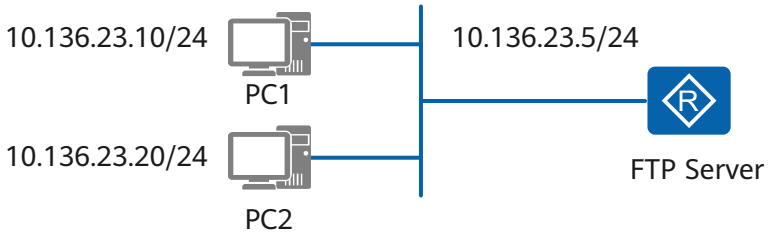
```
#
 sysname TFTP Client
#
return
```

11.6.3 Example for Managing Files When the Device Functions as an FTP Server

Networking Requirements

As shown in **Figure 11-2**, PC1 connects to the device, and the IP address of the management network interface on the device is 10.136.23.5. The device needs to be upgraded. The device is required to function as the FTP server to upload the system software from PC1 to the device and save the configuration file to PC1 for backup. A security policy is configured to ensure that only PC1 is allowed to access the FTP server.

Figure 11-2 Networking diagram for managing files when the device functions as an FTP server



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the FTP function and FTP user information including user name, password, user level, service type, and authorized directory on the FTP server.
2. Configure access permissions on the FTP server.
3. Save the **vrpcfg.zip** file on the FTP server.
4. Connect to the FTP server from the PC.
5. Upload **devicesoft.cc** to and download **vrpcfg.zip** from the FTP server.

Procedure

Step 1 Configure the FTP function and FTP user information on the FTP server.

```
<Huawei> system-view
[Huawei] sysname FTP_Server
[FTP_Server] ftp server enable
```

 Copyright © Huawei Technologies Co., Ltd.

```
[FTP_Server] aaa
[FTP_Server-aaa] local-user admin1234 password irreversible-cipher Helloworld@6789
[FTP_Server-aaa] local-user admin1234 privilege level 15
[FTP_Server-aaa] local-user admin1234 service-type ftp
[FTP_Server-aaa] local-user admin1234 ftp-directory flash:
[FTP_Server-aaa] quit
```

Step 2 Configure access permissions on the FTP server.

```
[FTP_Server] acl number 2001
[FTP_Server-acl-basic-2001] rule permit source 10.136.23.10 32
[FTP_Server-acl-basic-2001] rule deny source 10.136.23.20 32
[FTP_Server-acl-basic-2001] quit
[FTP_Server] ftp acl 2001
[FTP_Server] quit
```

Step 3 Save the **vrpcfg.zip** file on the FTP server.

```
<FTP_Server> save
```

Step 4 Connect to the FTP server from the PC as the **admin1234** user whose password is **Helloworld@6789** and transfer files in binary mode.

Assume that the PC runs the Window XP operating system.

```
C:\Documents and Settings\Administrator> ftp 10.136.23.5
Connected to 10.136.23.5.
220 FTP service ready.
User (10.136.23.5:(none)): admin1234
331 Password required for admin1234.
Password:
230 User logged in.
ftp> binary
200 Type set to I.
ftp>
```

Step 5 Upload **devicesoft.cc** to and download **vrpcfg.zip** from the FTP server.

Upload the **devicesoft.cc** file to the FTP server.

```
ftp> put devicesoft.cc
200 Port command okay.
150 Opening BINARY mode data connection for devicesoft.cc
226 Transfer complete.
ftp: 93832832 bytes sent in 136.34Seconds 560.79Kbytes/sec.
```

Download the **vrpcfg.zip** file.

```
ftp> get vrpcfg.zip
200 Port command okay.
150 Opening BINARY mode data connection for vrpcfg.zip.
226 Transfer complete.
ftp: 1257 bytes received in 0.03Seconds 40.55Kbytes/sec.
```

NOTE

The **devicesoft.cc** file to be uploaded and the **vrpcfg.zip** file to be downloaded are stored in the local directory on the FTP client. Before uploading and downloading files, obtain the local directory on the client. The default FTP user's local directory on the Windows XP operating system is **C:\Documents and Settings\Administrator**.

Step 6 Verify the configuration.

Run the **dir** command on the FTP server to check the **devicesoft.cc** file.

```
<FTP_Server> dir
Directory of flash:/

 Idx  Attr     Size(Byte)  Date        Time       FileName
   0  -rw-             14  Mar 13 2012 14:13:38   back_time_a
   1  drw-              -  Mar 11 2012 00:58:54   logfile
   2  -rw-              4  Nov 17 2011 09:33:58   snmpnotilog.txt
```

 Copyright © Huawei Technologies Co., Ltd.

```
  3  -rw-        11,238  Mar 12 2012 21:15:56   private-data.txt
  4  -rw-         1,257  Mar 12 2012 21:15:54   vrpcfg.zip
  5  -rw-            14  Mar 13 2012 14:13:38   back_time_b
  6  -rw-    93,832,832  Mar 13 2012 14:24:24   devicesoft.cc
  7  drw-             -  Oct 31 2011 10:20:28   sysdrv
  8  drw-             -  Feb 21 2012 17:16:36   compatible
  9  drw-             -  Feb 09 2012 14:20:10   selftest
 10  -rw-        19,174  Feb 20 2012 18:55:32   backup.cfg
 11  -rw-        23,496  Dec 15 2011 20:59:36   20111215.zip
 12  -rw-           588  Nov 04 2011 13:54:04   servercert.der
 13  -rw-           320  Nov 04 2011 13:54:26   serverkey.der
 14  drw-             -  Nov 04 2011 13:58:36   security
...
1,927,220 KB total (1,130,464 KB free)
```

Access the FTP user's local directory on the PC and check the **vrpcfg.zip** file.

----End

Configuration File

```
#
sysname FTP_Server
#
aaa
 local-user admin1234 password irreversible-cipher %^%#D2cW%k[R=*_*l"E^X9M6Ra'6D\iS(Xqg%U@4,I!
$zbBUa'9R%^%#
 local-user admin1234 privilege level 15
 local-user admin1234 ftp-directory flash:
 local-user admin1234 service-type ftp
#
interface GigabitEthernet1/0/0
 ip address 10.136.23.5 255.255.255.0
#
 acl number 2001
  rule 5 permit source 10.136.23.10 32
#
 ftp server enable
 ftp acl 2001
#
return
```

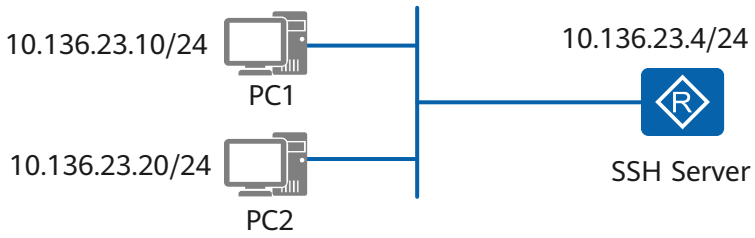
11.6.4 Example for Managing Files Using SFTP When the Device Functions as an SSH Server

Networking Requirements

As shown in **Figure 11-3**, PC1 connects to the device, and the IP address of the management network interface on the device is 10.136.23.4. Files need to be securely transferred between PC1 and the device. Configure the device as the SSH server to provide the SFTP service so that the SSH server can authenticate the client and encrypt data in bidirectional mode, ensuring secure file transfer. A security policy is configured to ensure that only PC1 is allowed to access the SSH server.

 Copyright © Huawei Technologies Co., Ltd.

Figure 11-3 Networking diagram for managing files using SFTP when the device functions as an SSH server



Configuration Roadmap

The configuration roadmap is as follows:

1. Generate a local key pair and enable the SFTP server function on the SSH server so that the server and client can securely exchange data.
2. Configure the VTY user interface on the SSH server.
3. Configure SSH user information including the authentication mode, user name, and password.
4. Configure access permissions on the SSH server to control SSH users.
5. Connect to the SSH server using the third-party software OpenSSH on the PC.

Procedure

Step 1 Generate a local key pair on the SSH server, and enable the SFTP server.

```
<Huawei> system-view
[Huawei] sysname SSH Server
[SSH Server] sftp server enable
[SSH Server] rsa local-key-pair create
The key name will be: Host
RSA keys defined for Host already exist.
Confirm to replace them? (y/n)[n]:y
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is less than 2048,
       It will introduce potential security risks.
Input the bits in the modulus[default = 2048]:2048
Generating keys...
.....+++
....+++
.....++++++++
.............++++++++
```

Step 2 Configure the VTY user interface on the SSH server.

```
[SSH Server] user-interface vty 0 14
[SSH Server-ui-vty0-14] authentication-mode aaa
[SSH Server-ui-vty0-14] protocol inbound ssh
[SSH Server-ui-vty0-14] quit
```

Step 3 Configure SSH user information including the authentication mode, user name, and password.

```
[SSH Server] aaa
[SSH Server-aaa] local-user client001 password irreversible-cipher Huawei@123
[SSH Server-aaa] local-user client001 privilege level 15
[SSH Server-aaa] local-user client001 service-type ssh
[SSH Server-aaa] quit
[SSH Server] ssh user client001 authentication-type password
```

 Copyright © Huawei Technologies Co., Ltd.

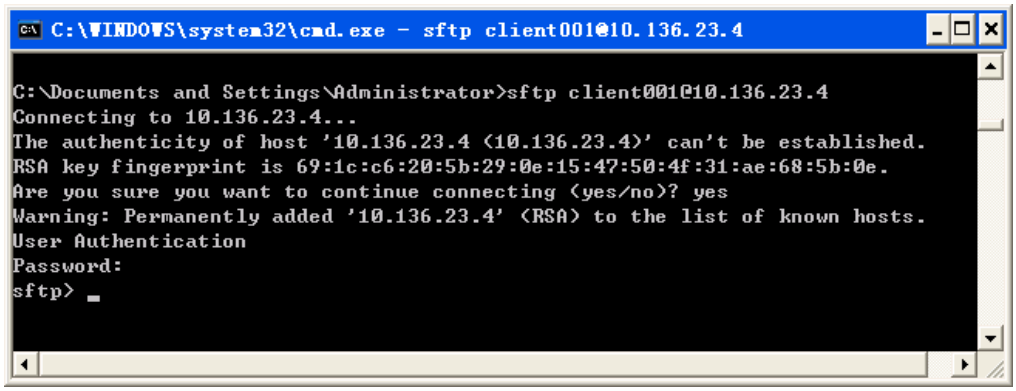
Step 4 Configure access permissions on the SSH server.

```
[SSH Server] acl 2001
[SSH Server-acl-basic-2001] rule permit source 10.136.23.10 32
[SSH Server-acl-basic-2001] rule deny source 10.136.23.20 32
[SSH Server-acl-basic-2001] quit
[SSH Server] user-interface vty 0 14
[SSH Server-ui-vty0-14] acl 2001 inbound
[SSH Server-ui-vty0-14] quit
```

Step 5 Connect to the SSH server using the third-party software OpenSSH on the PC.

The Windows CLI can identify OpenSSH commands only when the OpenSSH is installed on the PC.

Figure 11-4 Connecting to the SSH server



After you connect to the SSH server through third-party software, the SFTP view is displayed. Then you can perform file-related operations in the SFTP view.

----End

Configuration File

Configuration file of the SSH_Server

```
#
 sysname SSH Server
#
acl number 2001
 rule 5 permit source 10.136.23.10 0
 rule 10 deny source 10.136.23.20 0
#
aaa
 local-user client001 password irreversible-cipher %^%#<R<G9j0<_;@]`h@]TnCUuGP-1Za*%2i*k!
X<~Q4Ha1B0GP0u%^%#
 local-user client001 privilege level 15
 local-user client001 service-type ssh
#
 sftp server enable
#
user-interface vty 0 14
 acl 2001 inbound
 authentication-mode aaa
 protocol inbound ssh
#
return
```

 Copyright © Huawei Technologies Co., Ltd.

11.6.5 Example for Managing Files When the Device Functions as a TFTP Client

Networking Requirements

As shown in **Figure 11-5**, the remote device at 10.1.1.1/24 functions as the TFTP server. The device at 10.2.1.1/24 functions as the TFTP client. Routes between the device and the server are reachable.

The device needs to be upgraded. To upgrade the device, you must download system software **devicesoft.cc** from and upload the configuration file **vrpcfg.zip** to the TFTP server.

Figure 11-5 Networking diagram for managing files when the device functions as a TFTP client



Configuration Roadmap

The configuration roadmap is as follows:

1. Run the TFTP software on the TFTP server and configure the working directory.
2. Run TFTP commands to download **devicesoft.cc** from and upload **vrpcfg.zip** to the TFTP server.

Procedure

Step 1 Run the TFTP software on the TFTP server and configure the working directory. (For details, see related third-party documentation.)

Step 2 Run TFTP commands to download **devicesoft.cc** from and upload **vrpcfg.zip** to the TFTP server.

```
<Huawei> tftp 10.1.1.1 get devicesoft.cc
Info: Transfer file in binary mode.
Downloading the file from the remote TFTP server. Please wait...\
TFTP: Downloading the file successfully.
93832832 bytes received in 722 seconds.
<Huawei> tftp 10.1.1.1 put vrpcfg.zip
Info: Transfer file in binary mode.
Uploading the file to the remote TFTP server. Please wait...|
TFTP: Uploading the file successfully.
7717 bytes send in 1 second.
```

Step 3 Verify the configuration.

Run the **dir** command on the TFTP client to check the **devicesoft.cc** file.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> dir
Directory of flash:/

 Idx  Attr     Size(Byte)  Date       Time       FileName
   0  -rw-            14  Mar 13 2012 14:13:38   back_time_a
   1  drw-             -  Mar 11 2012 00:58:54   logfile
   2  -rw-             4  Nov 17 2011 09:33:58   snmpnotilog.txt
   3  -rw-        11,238  Mar 12 2012 21:15:56   private-data.txt
   4  -rw-         7,717  Mar 12 2012 21:15:54   vrpcfg.zip
   5  -rw-            14  Mar 13 2012 14:13:38   back_time_b
   6  -rw-    93,832,832  Mar 13 2012 14:24:24   devicesoft.cc
   7  drw-             -  Oct 31 2011 10:20:28   sysdrv
   8  drw-             -  Feb 21 2012 17:16:36   compatible
   9  drw-             -  Feb 09 2012 14:20:10   selftest
  10  -rw-        19,174  Feb 20 2012 18:55:32   backup.cfg
  11  -rw-        43,496  Dec 15 2011 20:59:36   20111215.zip
  12  -rw-           588  Nov 04 2011 13:54:04   servercert.der
  13  -rw-           320  Nov 04 2011 13:54:26   serverkey.der
  14  drw-             -  Nov 04 2011 13:58:36   security
...
1,927,220 KB total (1,130,464 KB free)
```

Access the working directory on the TFTP server and check the **vrpcfg.zip** file.

----End

11.6.6 Example for Managing Files When the Device Functions as an FTP Client

Networking Requirements

As shown in **Figure 11-6**, the remote device at 10.1.1.1/24 functions as the FTP server. The device at 10.2.1.1/24 functions as the FTP client. Routes between the device and the server are reachable.

The device needs to be upgraded. To upgrade the device, you must download system software **devicesoft.cc** from and upload the configuration file **vrpcfg.zip** to the FTP server.

Figure 11-6 Networking diagram for managing files when the device functions as an FTP client



Configuration Roadmap

The configuration roadmap is as follows:

1. Run the FTP software on the FTP server and configure FTP user information.
2. Connect to the FTP server.

 Copyright © Huawei Technologies Co., Ltd.

3. Run FTP commands to download **devicesoft.cc** from and upload **vrpcfg.zip** to the FTP server.

Procedure

Step 1 Run the FTP software on the FTP server and configure FTP user information. (For details, see related third-party documentation.)

Step 2 Connect to the FTP server.

```
<Huawei> ftp 10.1.1.1
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1.
220 FTP service ready.
User(10.1.1.1:(none)):admin
331 Password required for admin.
Enter password:
230 User logged in.

[Huawei-ftp]
```

Step 3 Run FTP commands to download **devicesoft.cc** from and upload **vrpcfg.zip** to the FTP server.

```
[Huawei-ftp] binary
[Huawei-ftp] get devicesoft.cc
[Huawei-ftp] put vrpcfg.zip
[Huawei-ftp] quit
```

Step 4 Verify the configuration.

Run the **dir** command on the FTP client to check the **devicesoft.cc** file.

```
<Huawei> dir
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time       FileName
    0  -rw-           14  Mar 13 2012 14:13:38   back_time_a
    1  drw-            -  Mar 11 2012 00:58:54   logfile
    2  -rw-            4  Nov 17 2011 09:33:58   snmpnotilog.txt
    3  -rw-       11,238  Mar 12 2012 21:15:56   private-data.txt
    4  -rw-        7,717  Mar 12 2012 21:15:54   vrpcfg.zip
    5  -rw-           14  Mar 13 2012 14:13:38   back_time_b
    6  -rw-   60,119,680  Mar 13 2012 14:24:24   devicesoft.cc
    7  drw-            -  Oct 31 2011 10:20:28   sysdrv
    8  drw-            -  Feb 21 2012 17:16:36   compatible
    9  drw-            -  Feb 09 2012 14:20:10   selftest
   10  -rw-       19,174  Feb 20 2012 18:55:32   backup.cfg
   11  -rw-       43,496  Dec 15 2011 20:59:36   20111215.zip
   12  -rw-          588  Nov 04 2011 13:54:04   servercert.der
   13  -rw-          320  Nov 04 2011 13:54:26   serverkey.der
   14  drw-            -  Nov 04 2011 13:58:36   security
...
468,304 KB total (208,272 KB free)
```

Access the working directory on the FTP server and check the **vrpcfg.zip** file.

----End

11.6.7 Example for Managing Files When the Device Functions as an SFTP Client

 Copyright © Huawei Technologies Co., Ltd.

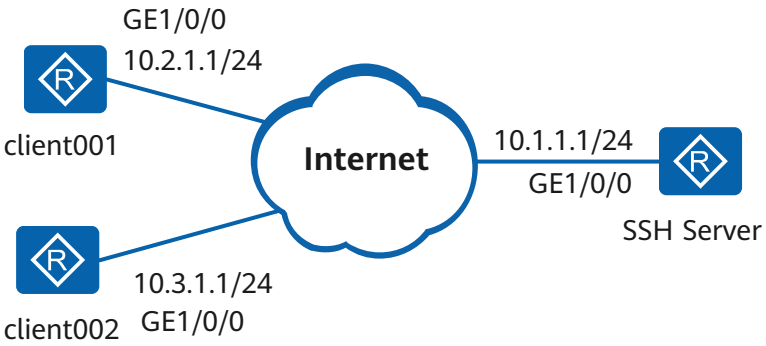
Networking Requirements

SSH secures file transfer on a traditional insecure network by authenticating the client and encrypting data in bidirectional mode. The client uses SFTP to securely connect to the SSH server and transfer files.

As shown in **Figure 11-7**, routes between the SSH server and clients client001 and client002 are reachable. In this example, Huawei device functions as an SSH server.

Client001 connects to the SSH server using the password authentication mode, and client002 using the RSA authentication mode.

Figure 11-7 Networking diagram for managing files when the device functions as an SFTP client



Configuration Roadmap

The configuration roadmap is as follows:

1. Generate a local key pair and enable the SFTP server function on the SSH server so that the server and client can securely exchange data.
2. Create users **client001** and **client002** and set their authentication modes on the SSH server.
3. Generate a local key pair on client002 and configure the RSA public key of client002 on the SSH server so that the server can authenticate the client when the client connects to the server.
4. Log in to the SSH server as users **client001** and **client002** using SFTP and manage files.

Procedure

Step 1 Generate a local key pair and enable the SFTP server function on the SSH server.

```
<Huawei> system-view
[Huawei] sysname SSH Server
[SSH Server] sftp server enable
[SSH Server] rsa local-key-pair create
The key name will be: Host
RSA keys defined for Host already exist.
Confirm to replace them? (y/n)[n]:y
The range of public key size is (512 ~ 2048).
```

 Copyright © Huawei Technologies Co., Ltd.

```
NOTES: If the key modulus is less than 2048,
       It will introduce potential security risks.
Input the bits in the modulus[default = 2048]:2048
Generating keys...
.....................................................................................+++
....+++
.....................................+++++++++
.............+++++++++
```

Step 2 Create SSH users on the SSH server.

Configure the VTY user interface.

```
[SSH Server] user-interface vty 0 4
[SSH Server-ui-vty0-4] authentication-mode aaa
[SSH Server-ui-vty0-4] protocol inbound ssh
[SSH Server-ui-vty0-4] user privilege level 3
[SSH Server-ui-vty0-4] quit
```

Create the **client001** user and set the authentication mode to **password** for the user.

```
[SSH Server] aaa
[SSH Server-aaa] local-user client001 password irreversible-cipher Helloworld@6789
[SSH Server-aaa] local-user client001 service-type ssh
[SSH Server-aaa] local-user client001 privilege level 3
[SSH Server-aaa] quit
[SSH Server] ssh user client001 authentication-type password
```

Create an SSH user **client002** and set the authentication mode to **rsa** for the user.

```
[SSH Server] aaa
[SSH Server-aaa] local-user client002 password irreversible-cipher Helloworld@6789
[SSH Server-aaa] local-user client002 service-type ssh
[SSH Server-aaa] local-user client002 privilege level 3
[SSH Server-aaa] quit
[SSH Server] ssh user client002 authentication-type rsa
```

Step 3 Generate a local key pair on client002 and configure the RSA public key of client002 on the SSH server.

Generate a local key pair on client002.

```
<Huawei> system-view
[Huawei] sysname client002
[client002] rsa local-key-pair create
The key name will be: Host
RSA keys defined for Host already exist.
Confirm to replace them? (y/n)[n]:y
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is less than 2048,
       It will introduce potential security risks.
Input the bits in the modulus[default = 2048]:2048
Generating keys...
.....................................................................................+++
....+++
.....................................+++++++++
.............+++++++++
```

Check the RSA public key of the client.

```
[client002] display rsa local-key-pair public

=================================================
Time of Key pair created: 2012-08-06 17:17:37+00:00
Key name: Host
Key type: RSA encryption Key
```

 Copyright © Huawei Technologies Co., Ltd.

```
=====================================================
Key code:
30820109
  02820100
    CB0E88EC A1C2CFEA F97126F9 36919C08 0455127B
    A3A48594 69517096 35626F55 E4FAF0EB FDA2B9E9
    5E417B2B E09F38B0 D26FCA73 FE2E3FC4 DFBEC8CF
    4ED0C909 E8D975E6 FFC73C81 D13FE71E 759DC805
    B0F0E877 4FC9288E BE1E197C 2A7186B0 B56F5573
    3A5EA588 29C63E3B 20D56233 8E63278D F941734F
    6B359C69 BBAE5A52 EB842179 04B4204D 5DB31D72
    97F0C085 DA771F66 0AAADC28 D264CEB9 5BADA92C
    CDE9F116 D6D99C48 CEBA3A1D 868B053A 32941D85
    CCAA9796 A4B55760 0A8108ED DB45DA12 F61634C9
    59431600 341FEDEF 5379D565 A8D1953D DEA018A2
    72F99FFC 63DE04BF 2A6219BD DF13D705 27D63DEF
    83D556BC 5B44D983 8D5EA126 C1EB71CB
  0203
    010001

=====================================================
Time of Key pair created: 2012-08-06 17:17:44+00:00
Key name: Server
Key type: RSA encryption Key
=====================================================
Key code:
3067
  0260
    DF8AFF3C 28213B94 2292852E E98657EE 11DE5AF4
    8A176878 CDD4BD31 55E05735 3080F367 A83A9034
    47D534CA 81250C1D 35401DC3 464E9E5F A50202CF
    A7AD09CD AC3F531C A763F0A0 4C8E51B9 18755400
    76AF4A78 225C92C3 01FE0DFF 06908363
  0203
    010001
```

Configure the RSA public key on the SSH server. (Information in bold in the **display** command output is the RSA public key. Copy the information to the server.)

```
[SSH Server] rsa peer-public-key rsakey001
[SSH Server-rsa-public-key] public-key-code begin
[SSH Server-rsa-key-code] 30820109
[SSH Server-rsa-key-code] 02820100
[SSH Server-rsa-key-code] CB0E88EC A1C2CFEA F97126F9 36919C08 0455127B
[SSH Server-rsa-key-code] A3A48594 69517096 35626F55 E4FAF0EB FDA2B9E9
[SSH Server-rsa-key-code] 5E417B2B E09F38B0 D26FCA73 FE2E3FC4 DFBEC8CF
[SSH Server-rsa-key-code] 4ED0C909 E8D975E6 FFC73C81 D13FE71E 759DC805
[SSH Server-rsa-key-code] B0F0E877 4FC9288E BE1E197C 2A7186B0 B56F5573
[SSH Server-rsa-key-code] 3A5EA588 29C63E3B 20D56233 8E63278D F941734F
[SSH Server-rsa-key-code] 6B359C69 BBAE5A52 EB842179 04B4204D 5DB31D72
[SSH Server-rsa-key-code] 97F0C085 DA771F66 0AAADC28 D264CEB9 5BADA92C
[SSH Server-rsa-key-code] CDE9F116 D6D99C48 CEBA3A1D 868B053A 32941D85
[SSH Server-rsa-key-code] CCAA9796 A4B55760 0A8108ED DB45DA12 F61634C9
[SSH Server-rsa-key-code] 59431600 341FEDEF 5379D565 A8D1953D DEA018A2
[SSH Server-rsa-key-code] 72F99FFC 63DE04BF 2A6219BD DF13D705 27D63DEF
[SSH Server-rsa-key-code] 83D556BC 5B44D983 8D5EA126 C1EB71CB
[SSH Server-rsa-key-code] 0203
[SSH Server-rsa-key-code] 010001
[SSH Server-rsa-key-code] public-key-code end
[SSH Server-rsa-public-key] peer-public-key end
```

Bind the **client002** user to the RSA public key of client002.

```
[SSH Server] ssh user client002 assign rsa-key rsakey001
```

Step 4 Connect SFTP clients to the SSH server.

If the clients connect to the SSH server for the first time, enable the initial authentication function on the clients.

 Copyright © Huawei Technologies Co., Ltd.

Enable the initial authentication function on client001.

```
<Huawei> system-view
[Huawei] sysname client001
[client001] ssh client first-time enable
```

Enable the initial authentication function on client002.

```
[client002] ssh client first-time enable
```

Log in to the SSH server from client001 in password authentication mode.

```
[client001] sftp 10.1.1.1
Please input the username: client001
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1 ...
 Continue to access it? [Y/N]:y
 [Y/N]:y
The server's public key will be saved with the name 10.1.1.1. Please wait.
..

Enter password:
sftp-client>
```

Log in to the SSH server from client002 in RSA authentication mode.

```
[client002] sftp 10.1.1.1
Please input the username: client002
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1 ...
 Continue to access it? [Y/N]:y
 [Y/N]:y
The server's public key will be saved with the name 10.1.1.1. Please wait.
..

sftp-client>
```

Step 5 Verify the configurations.

Run the **display ssh server status** command. You can see that the SFTP service has been enabled. Run the **display ssh user-information** command. Information about the configured SSH users is displayed.

Check the SSH server status.

```
[SSH Server] display ssh server status
 SSH version                     :1.99
 SSH connection timeout          :60 seconds
 SSH server key generating interval  :0 hours
 SSH Authentication retries      :3 times
 SFTP Server                     :Enable
 Stelnet server                  :Disable
```

Check information about SSH users.

```
[SSH Server] display ssh user-information
 ------------------------------------------------------------------------------
 Username        Auth-type         User-public-key-name
 ------------------------------------------------------------------------------
 client001       password          null
 client002       rsa               rsakey001
 ------------------------------------------------------------------------------
```

----End

 Copyright © Huawei Technologies Co., Ltd.

Configuration Files

- Configure file on the SSH server

```
#
sysname SSH Server
#
 rsa peer-public-key rsakey001
  public-key-code begin
   30820109
     02820100
       CB0E88EC A1C2CFEA F97126F9 36919C08 0455127B A3A48594 69517096 35626F55
       E4FAF0EB FDA2B9E9 5E417B2B E09F38B0 D26FCA73 FE2E3FC4 DFBEC8CF 4ED0C909
       E8D975E6 FFC73C81 D13FE71E 759DC805 B0F0E877 4FC9288E BE1E197C 2A7186B0
       B56F5573 3A5EA588 29C63E3B 20D56233 8E63278D F941734F 6B359C69 BBAE5A52
       EB842179 04B4204D 5DB31D72 97F0C085 DA771F66 0AAADC28 D264CEB9 5BADA92C
       CDE9F116 D6D99C48 CEBA3A1D 868B053A 32941D85 CCAA9796 A4B55760 0A8108ED
       DB45DA12 F61634C9 59431600 341FEDEF 5379D565 A8D1953D DEA018A2 72F99FFC
       63DE04BF 2A6219BD DF13D705 27D63DEF 83D556BC 5B44D983 8D5EA126 C1EB71CB
     0203
       010001
  public-key-code end
 peer-public-key end
#
aaa
 local-user client001 password irreversible-cipher %^%#HW=5%Mr;:2)/RX$FnU1HLO%-TBMp4wn%;~
\#%iAut}_~O%0L%^%#
 local-user client001 privilege level 3
 local-user client001 service-type ssh
 local-user client002 password irreversible-cipher %^%#*~Br";[g6Pv5Zf>$~{hY+N!`{$<[Y{;l02P)B,EBz
\1FN!c+%^%#
 local-user client002 privilege level 3
 local-user client002 service-type ssh
#
 ssh user client002 assign rsa-key rsakey001
 ssh user client002 authentication-type rsa
 sftp server enable
#
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 3
 protocol inbound ssh
#
return
```

- Configuration file on client001

```
#
 sysname client001
#
ssh client first-time enable
#
return
```

- Configuration file on client002

```
#
 sysname client002
#
ssh client first-time enable
#
return
```

11.7 Troubleshooting System Startup

11.7.1 FTP Login Failure

 Copyright © Huawei Technologies Co., Ltd.

Cause Analysis

- The FTP server is not running.
- The listening port number of the FTP server is not the default one, and no port number is specified when you log in to the FTP server.
- The authentication information, authorized directory, and user level of the FTP user are not configured.
- The number of online FTP users who have logged in to the FTP server reaches the upper threshold 5.
- An ACL is configured on the FTP server, and the FTP client IP address is not specified in the ACL.

Procedure

Step 1 Check whether the FTP server is running properly.

Run the **display ftp-server** command in any view to check the FTP server status.

- The following information indicates that the FTP server is not running:

```
<Huawei> display ftp-server
Info: The FTP server is already disabled.
```

  Run the **ftp server enable** command in the system view to start the FTP server.

```
<Huawei> system-view
[Huawei] ftp server enable
Info: Succeeded in starting the FTP server.
```

- The following information indicates that the FTP server is running properly:

```
<Huawei> display ftp-server
  FTP server is running
  Max user number              5
  User count                   0
  Timeout value(in minute)     30
  Listening port               21
  Acl number                   0
  FTP server's source address  0.0.0.0
```

Step 2 Check whether the listening port number of the FTP server is the default port number 21.

1. Run the **display tcp status** command in any view to check the current TCP port listening status.

```
<Huawei> display tcp status
TCPCB     Tid/Soid Local Add:port       Foreign Add:port      VPNID  State
2a67f47c  6  /1    0.0.0.0:21          0.0.0.0:0             23553  Listening
2b72e6b8  115/4    0.0.0.0:22          0.0.0.0:0             23553  Listening
3265e270  115/1    0.0.0.0:23          0.0.0.0:0             23553  Listening
2a6886ec  115/23   10.137.129.27:23    10.138.77.43:4053     0      Establish
ed
2a680aac  115/14   10.137.129.27:23    10.138.80.193:1525    0      Establish
ed
2a68799c  115/20   10.137.129.27:23    10.138.80.202:3589    0      Establish
ed
```

2. Run the **display ftp-server** command in any view to check the listening port number of the FTP server.

```
<Huawei> display ftp-server
  FTP server is running
  Max user number              5
  User count                   0
  Timeout value(in minute)     30
  Listening port               21
```

 Copyright © Huawei Technologies Co., Ltd.

```
Acl number                  0
FTP server's source address 0.0.0.0
```

If the listening port number is not 21, run the **ftp server port** command to set the listening port number to 21.

```
<Huawei> system-view
[Huawei] undo ftp server
Info: Succeeded in closing the FTP server.
[Huawei] ftp server port 21
[Huawei] ftp server enable
Info: Succeeded in starting the FTP server.
```

Alternatively, enter the port number configured on the server when you set up an FTP connection on the FTP client.

Step 3 Check whether the authentication information, authorized directory, and user level of the FTP user are correctly configured.

The FTP user name, password, authorized directory, and user level must be configured. If the FTP authorized directory and user level are not configured, login fails.

1. Run the **aaa** command to enter the AAA view.
2. Run the **local-user** *user-name* **password irreversible-cipher** *password* command to configure the local FTP user name and password.
3. Run the **local-user** *user-name* **ftp-directory** *directory* command to specify an FTP authorized directory for the FTP user.
4. Run the **local-user** *user-name* **privilege level** *level* command to set the FTP user level. The user level must be set to **3** or higher to ensure successful connection establishment.

The service type is optional. By default, the system does not support any service type.

Run the **local-user** *user-name* **service-type ftp** command to set the service types for the FTP user.

Step 4 Check whether the number of online FTP users who have logged in to the FTP server reaches the upper threshold.

Run the **display ftp-users** command to check the number of online FTP users.

Step 5 Check the ACL rule on the FTP server.

Run the **display** [**ipv6**] **ftp-server** command to check the ACL rule on the FTP server.

If an ACL is configured on the FTP server, only IP addresses specified in the ACL can log in to the FTP server.

----End

11.7.2 Failure in Uploading Files to the FTP Server

Cause Analysis

- The FTP source or destination directory name consists of unsupported characters.

 Copyright © Huawei Technologies Co., Ltd.

- The storage space of the FTP root directory is insufficient.

Procedure

Step 1 Check whether the FTP source and destination directory names consist of unsupported characters.

The following characters and spaces are not supported: ~ */ \ : ' "

If the directory names consist of any unsupported characters, modify the directory names.

Step 2 Check whether the storage space of the FTP root directory is sufficient.

Run the **dir** command on the FTP server to check the free space of the FTP root directory.

If the space of the FTP root directory is insufficient, run the **delete /unreserved** command in the user view to delete unnecessary files.

----End

11.8 FAQ About File Management

This section describes common problems that may occur during the configuration and their solutions.

11.8.1 Does an AR Router Support Resumable FTP Download?

In versions earlier than V200R006C10, an AR router does not support resumable FTP download.

In V200R006C10 and later versions, if the router functions as an FTP client and downloads a file from the FTP server, the router supports resumable download. If the router is powered off during the download process, the file may be damaged. If you need to resume the download after the router restarts, you are advised to use the newly downloaded file to overwrite the originally downloaded file, or delete the originally downloaded file and re-download the file. Otherwise, the download may fail.

NOTE

Resumable FTP download takes effect for only one file. If you need to resume the download when the content of the target file changes, you are advised to use the newly downloaded file to overwrite the originally downloaded file, or delete the originally downloaded file and re-download the file. Otherwise, the file content may be incorrect.

11.8.2 How Many FTP Users Can Log In to a Router Simultaneously?

Five FTP users can log in to a router simultaneously.

 Copyright © Huawei Technologies Co., Ltd.

11.8.3 Why Does the Available Space on a Storage Medium Not Change After a File Is Deleted?

If you specify the **/unreserved** parameter when running the **delete** [**/unreserved**] [**/force**] { *filename* | *devicename* } command to delete a specified file on a storage medium, the file is deleted permanently and cannot be restored.

If you do not specify the **/unreserved** parameter when running the **delete** [**/unreserved**] [**/force**] { *filename* | *devicename* } command to delete a specified file on a storage medium, the file is moved to the recycle bin and is not deleted permanently. The file still occupies storage space on the storage medium.

You can run the **dir /all** command to view information about all files, including deleted files marked with square brackets ([ ]). To restore deleted files, run the **undelete** { *filename* | *devicename* } command.

To remove a file from the recycle bin to release the occupied storage space, run the **reset recycle-bin** [*filename* | *devicename*] command.

 Copyright © Huawei Technologies Co., Ltd.

12 Configuring System Startup

About This Chapter

This chapter describes how to configure system startup.

Context

The AR100&AR120&AR150&AR160&AR200&AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204E-D-27GE, AR2204-24GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-48GE-P, AR2204E, AR2204E-D, AR2204-51GE, AR2204-51GE-R, AR2220L-DC, AR2220L-AC and AR3670 support the flash memory and USB flash drive. The AR2220-AC, AR2220-DC, AR2220E, AR2240C support the flash memory, hard disk and USB flash drive. The AR2204, AR2240 and AR3260 (using SRU40, SRU60, SRU80, SRU100, SRU100E, SRU200E, SRU200 and SRU400) support the flash memory, Micro SD card, and USB flash drive. The AR2240, AR2204XE-DC and AR2204XE support the Micro SD card and USB flash drive.

NOTE

If the USB flash drive contains activated system software or patch software, the USB flash drive is a key component of the system and cannot be removed.

In this chapter, the Micro SD card is used as an example of the storage device.

12.1 Overview of System Startup

12.2 Licensing Requirements and Limitations for System Startup
This section provides the configuration precautions of configuring System Startup.

12.3 Managing Configuration Files

12.4 Configuring System Startup Files

12.5 Restarting the Device

12.6 Configuration Examples for System Startup

 Copyright © Huawei Technologies Co., Ltd.

12.1 Overview of System Startup

The system loads the system software and configuration file during a startup. If a patch file is specified for next startup, the system also loads the specified patch file.

System startup scenarios are as follows:

- Version upgrade: Upgrade the system software to a later version.

  To add new features, optimize existing features, or solve problems in the current version, you need to upgrade the device. To upgrade the device, load the upgrade system software and restart the device.

- Version rollback: Degrade the software to an earlier version.

  If an error occurs after the upgrade, perform version rollback to restore normal service operating. You need to load earlier version system software and restart the device.

- First startup: When a new device is deployed on a network, you can load an existing configuration file on the device to meet user needs.

  A new device contains only factory configurations. To connect a new device to the network and deploy services on it, you have to spend a lot of time on device configuration. To save time on device configuration, specify a configuration file that meets user needs for the device and restart the device.

- Patch update: Specify the patch file to be loaded after an upgrade.

  You can specify a new patch file when upgrading the device. The patch takes effect immediately when the upgrade is complete.

NOTE

- The upgrade of a device is closely related to the released software versions. The corresponding upgrade guide is released with each new version and you can upgrade the device according to the guide. To obtain the upgrade guides, visit **https://support.huawei.com/enterprise** and download the upgrade guide based on the product name and version.
- When the message "Start Memory Test ? ('t' or 'T' is test):" is displayed during the device startup, you can press **T** to start the memory detection.
- For details about commands used for device upgrade, see "Basic Configurations Commands - Upgrade Commands" in the *Huawei AR Series Access Routers Command Reference*.

System Software

The device software includes BootROM software and system software. After the device is powered on, it runs the BootROM software to initialize the hardware and display the hardware parameters. Then the device runs the system software. The system software provides drivers and adaptation functions for hardware, and offers services features. The BootROM software and system software are prerequisite for device startup and operation, providing support, management, and services for the device.

A device upgrade includes BootROM software upgrade and system software upgrade.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The BootROM software is included in the system software package (.cc file) of the device. The BootROM software is automatically upgraded in system software upgrade.

Configuration File

A configuration file is a collection of command lines. The current configurations are saved in configuration files, and continue to take effect after the device restarts. You can view configurations in configuration files or upload the files to other devices to implement batch configuration.

A configuration file is in the text format and meets the following requirements:

- The configuration file saves configuration commands.
- Only non-default parameters are stored in the configuration file, which saves the space.
- The commands used in the same command view form a section. Sections are separated by comment lines beginning with comment signs (#). The command under a comment sign is run in the system view. There can be one or multiple comment lines.
- Sections are arranged in order of global configurations, interface-based configurations, protocol configurations, and user interface configurations.
- The configuration file name extension must be .cfg or .zip. In addition, the configuration file must be saved to the root directory of the storage device.

The following table describes the factory configuration, configuration file and current configuration.

Concept	Description	Command
Factory configuration	The device is delivered with basic configurations so that it can start and work properly when there is no configuration file or the configuration file is lost or damaged. These configurations are called factory configurations.	Run the **display factory-configuration** command to check the factory configurations of the device.
Configuration file	When the device is powered on, the device reads the configuration file from the default directory to boot the system. Therefore, the configuration in the file is called the initial configuration. If no configuration file is stored in the default directory, the device uses the default parameters for initialization.	• Run the **display startup** command to check the current and next startup configuration files. • Run the **display saved-configuration** command to check the configuration file for next startup.

 Copyright © Huawei Technologies Co., Ltd.

Concept	Description	Command
Current configuration	The configurations that are valid during the device running are called current configurations.	Run the **display current-configuration** command to check the current configuration.

If you modify the current configuration and want to use the modified configuration as the next startup configuration, run the **save** command to save the new configuration to the default storage device.

NOTE

If a command in incomplete form is configured, the system saves the command to the configuration file in its complete form, which may cause the command to have more than 510 characters. (The maximum length of a command supported by the system is 510 characters.) The incomplete command cannot be recovered after the system restarts.

Patch File

A patch is a kind of software compatible with the system software. It is used to remove a few issues in the software that need to be solved immediately. Patches can also fix errors or improve adaptation of the system software. For example, patches can fix defects of the system and optimize some functions to meet service requirements.

The patches are released in patch files. A patch file may contain one or more patches with different functions. When patch files are loaded from the storage device to the patch area in the memory, they are assigned unique sequence number for users to identify, manage, and operate the patches.

Patch classification

According to impact on services, patches can be classified into hot patch and cold patch.

- Hot patch (HP): The services are not interrupted when the HP is loaded and activated, which reduces upgrade costs and eliminates upgrade risks.
- Cold Patch (CP): You must restart the device for the CP to take effect. Services are interrupted during the restart.

According to patch dependency, patches can be classified into incremental and non-incremental patches.

- An incremental patch is dependent on previous patches. A new patch file contains all the patch information in the previous patch file. You can install the patch file without uninstalling the original patch file.
- A non-incremental patch is exclusive in the current system. To install another patch file when there is already one, uninstall the existing patch file, and then install and run the new patch file.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The currently released patches are hot patches and incremental patches. All the patches mentioned in the subsequent sections are hot patches and incremental patches unless otherwise specified.

Status of Patches

Each patch has its own state that can only be changed with command line.

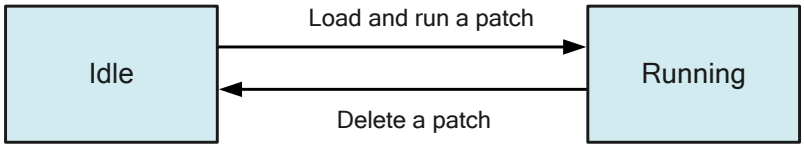
Table 12-1 describes the patch status.

Table 12-1 Status of patches

Status	Description	Patch Status Transition
Idle	The patch file is saved to the storage device but has not been loaded to the patch area.	When a patch in the storage device is loaded to the patch area, the patch is in the running state.
Running	When a patch is stored in the patch area and runs permanently, the patch is in the running state. If a board is reset, the running patch on the board remains in the running state.	You can unload the patch that is in the running state so that it can be deleted from the patch area.

Figure 12-1 shows patch status transition.

Figure 12-1 Patch status transition



Installing Patches

Installing patches is a way of upgrading a device. Patches can be installed in the following ways:

- The hot patches are generally installed while the device is running without interrupting services. This is an advantage of hot patches.

  For details on how to install patches, see the corresponding patch installation guide. For details about commands used for device upgrade, see "Basic Configurations Commands - Upgrade Commands" in the *Huawei AR Series Access Routers Command Reference*.

 Copyright © Huawei Technologies Co., Ltd.

- Another way is to specify a patch file for next startup, which is described in this chapter. The patch file takes effect after the device reboots. The method is often used during a system upgrade.

12.2 Licensing Requirements and Limitations for System Startup

This section provides the configuration precautions of configuring System Startup.

Involved Network Elements

None

Licensing Requirements

configuring System Startup is a basic feature of a router and is not under license control.

Feature Limitations

Creating and modifying the configuration file locally are not recommended because the file format may be incorrect. As a result, configuration restoration will fail.

12.3 Managing Configuration Files

Pre-configuration Tasks

You can perform operations such as saving the configuration file and backing up the configuration file.

Before managing configuration files, complete the following task:

- Log in to the device.

Configuration Process

Perform one or multiple of the following tasks:

12.3.1 Saving the Configuration File

Context

You can run commands to modify the current configuration of the device, but the modified configuration will be lost after the device restarts. To enable the new configuration to still take effect after a restart, save the current configuration in the configuration file before restarting the device. Use either of the following methods to save the current configuration:

- Configure the automatic save function.

 Copyright © Huawei Technologies Co., Ltd.

- Manually save the configuration.

Procedure

- Save the configurations automatically.

  NOTICE

  If an interface board is not running, related configurations may be lost when the system automatically saves the configuration file.

  The **autosave interval** command cannot be used together with the **autosave time** command.

  - Run **autosave interval** *value*

    Automatic saving of configurations is enabled.

    By default, automatic saving of configurations is disabled. The *value* parameter can be set to **on** or **off**. The value **on** enables automatic saving of configurations, and the value **off** disables this function.
  - Run **autosave interval** { *time* | **configuration** *time* }

    The system is configured to save the configurations at a specified interval.

    If **interval** *time* is specified, the system saves the configurations at the specified interval regardless of whether the configuration is changed.

    - The default interval is 0 seconds, indicating that the system does not save the configurations automatically.
    - After the automatic save function is enabled, the default interval is 30 minutes if *time* is not specified.
  - Run **autosave time** { *value* | *time-value* }

    The system is configured to save the configurations at a specified time.

    When the automatic save function is enabled, the modified configuration is saved at the specified time. When the automatic save function is disabled, the system does not save the configurations automatically and you need to manually save the modified configuration.

  NOTE

  In automatic save mode, the system automatically saves configurations to the current startup configuration file. You can run the **display startup** command to check the name of the current startup configuration file.

- Save the configurations manually.
  - Run **save** [**all**] [*configuration-file*]

    The current configuration is saved.

    The configuration file name extension must be .zip or .cfg. The system startup file must be stored in the root directory of the storage device.

    Run the **save all** command to save all the current configurations, including the configurations of the boards that are not running, to the current storage directory.

 Copyright © Huawei Technologies Co., Ltd.

- If you do not specify *configuration-file* when saving the configuration file for the first time, the system asks you whether to save the configuration file as **vrpcfg.zip**.
- If you do not specify *configuration-file*, configurations are saved to the current startup configuration file. You can run the **display startup** command to check the name of the current startup configuration file.
- You can run the **pwd (user view)** command in the user view to check the current storage directory.
- You can run the **cd (user view)** command in the user view to modify the current storage directory.

----End

12.3.2 Comparing Configuration Files

Context

You can compare the current configuration file with the next startup configuration file to check whether they are consistent and determine whether to set the current configuration file as the next startup configuration file.

The system displays the different content starting from the first different character to the end of the file. By default, the system displays 120 characters. If the different content contains less than 120 characters, the system displays only the content from the first different character to the end of the file.

If the next startup configuration file is unavailable or empty, the system displays a message indicating that the files fail to be read.

NOTE

The configuration file name extension must be .cfg or .zip.

Procedure

- Run **compare configuration** [*configuration-file* [*current-line-number save-line-number*]]

  The system starts to check whether the current configurations are identical with the next startup configuration file or the specified configuration file.

  If parameters are not specified, the configuration files are compared from the first line. The parameters *current-line-number* and *save-line-number* are used to continue the comparison, neglecting the differences, after differences are found.

----End

 Copyright © Huawei Technologies Co., Ltd.

12.3.3 Backing Up the Configuration File

Context

If the device is damaged unexpectedly, the configuration file cannot be recovered. You can back up the configuration file in advance using one of the following methods:

- Copy the content in the display on the screen.
- Back up the configuration file to the storage device.
- Back up the configuration file using FTP, TFTP, or SFTP.

Procedure

- Copying the content in the display on the screen

  Run the **display current-configuration** command and copy all command outputs to a .txt file. The configuration file is backed up in the hard disk of the maintenance terminal.

  NOTE

  If a configuration is too long, it may be displayed in two lines on the terminal screen, depending on the terminal software. When copying a two-line configuration from the screen to a .txt file, ensure that the configuration is displayed in only one line. Otherwise, configuration restoration may fail when the .txt file is used.

- Backing up the configuration file to the storage device

  The current configuration file can be backed up immediately to the SD card of the device. After the device starts, run the following commands to back up the configuration file to the SD card of the device:

  ```
  <Huawei> save config.cfg
  <Huawei> copy config.cfg backup.cfg
  ```

  To save the configuration in a directory other than the default storage device, specify an absolute path.

- Backing up the configuration file using FTP, TFTP, or SFTP

  The device supports configuration file backup through FTP, TFTP, or SFTP. Configuration file backup through FTP or TFTP is simple, but there are security risks. In scenarios with high security requirements, configuration file backup through SFTP is recommended. The following describes the configuration file backup process using FTP as an example. For details about TFTP and SFTP, see "File Management" in *Huawei AR Series Access Routers Configuration Guide - Basic Configurations*.

  a. Start the FTP service when the device works as the FTP server.

     Enable the FTP server function on the device. Create an FTP user with the name **huawei** and password **Helloworld@6789**. The user is authorized to access the sd1 directory.

     ```
     <Huawei> system-view
     [Huawei] ftp server enable
     Info: Succeeded in starting the FTP server.
     [Huawei] aaa
     [Huawei-aaa] local-user huawei password irreversible-cipher Helloworld@6789
     [Huawei-aaa] local-user huawei ftp-directory sd1:
     ```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-aaa] local-user huawei service-type ftp
[Huawei-aaa] local-user huawei privilege level 15
```

b. On the maintenance terminal, initiate an FTP connection to the device.

On the PC, set up an FTP connection to the device through the FTP client. Assume that the device IP address is 10.110.24.254.

```
C:\Documents and Setting\Administrator> ftp 10.110.24.254
Connected to 10.110.24.254.
220 FTP service ready.
User (10.110.24.254:(none)): huawei
331 Password required for huawei.
Password:
230 User logged in.
```

c. Configure transfer parameters.

If the FTP user is authenticated, the FTP client displays the prompt character of **ftp>**. Enter **binary** following the prompt character, and specify the path c:\temp the uploaded file is to be saved on the FTP client.

```
ftp> binary
200 Type set to I.
ftp> lcd c:\temp
Local directory now C:\temp.
```

d. Transfer the configuration file.

On the PC, run the **get** command to load the configuration file to the specified path and save the file as **backup.cfg**.

```
ftp> get config.cfg backup.cfg
```

e. Check whether the **config.cfg** and **backup.cfg** files have the same size. If they have the same size, the backup is successful.

----End

12.3.4 Recovering the Configuration File

Context

When incorrect configurations are performed and functions are abnormal, you can use one of the following methods:

- Recover the configuration file that is backed up in the storage device.
- Recover the configuration file using FTP, TFTP, or SFTP.

NOTE

After recovering the configuration file, you must restart the device to make the file take effect. Run the **startup saved-configuration** command to specify the next startup configuration file. If the configuration file name is unchanged, you do not need to run this command. Run the **reboot** command to restart the device. When **Warning: All the configuration will be saved to the next startup configuration. Continue? [y/n]:** is displayed, enter **n** to prevent the current configurations of the device from being saved to the backup configuration file.

Procedure

- Recover the configuration file that is backed up in the SD card.

 Copyright © Huawei Technologies Co., Ltd.

This step recovers the backup configuration file stored in the SD card of the device to the current system configuration file. When the device is working properly, run the following command:

a. Recover the backup configuration file stored in the SD card of the device to the current system configuration file.

```
<Huawei> startup saved-configuration backup.cfg
```

b. Restart the device. The configuration file recovery is complete.

```
<Huawei> reboot
Info: The system is comparing the configuration, please wait.
Warning: All the configuration will be saved to the next startup configuration. Continue? [y/n]: n
System will reboot! Continue? [y/n]: y
Info: system is rebooting ,please wait...
```

- Recover the configuration file using FTP, TFTP, or SFTP

  The device supports configuration file recovery through FTP, TFTP, or SFTP. Configuration file recovery through FTP or TFTP is simple, but there are security risks. In scenarios with high security requirements, configuration file recovery through SFTP is recommended. The following describes how to recover the configuration file that is backed up on a PC through FTP. For details about TFTP and SFTP, see "File Management" in *Huawei AR Series Access Routers Configuration Guide - Basic Configurations*.

  a. Start the FTP service when the device works as the FTP server.

     Enable the FTP server function on the device. Create an FTP user with the name **huawei** and password **Helloworld@6789**. The user is authorized to access the sd1 directory.

```
<Huawei> system-view
[Huawei] ftp server enable
Info: Succeeded in starting the FTP server.
[Huawei] aaa
[Huawei-aaa] local-user huawei password irreversible-cipher Helloworld@6789
[Huawei-aaa] local-user huawei ftp-directory sd1:
[Huawei-aaa] local-user huawei service-type ftp
[Huawei-aaa] local-user huawei privilege level 15
```

  b. On the maintenance terminal, initiate an FTP connection to the device.

     On the PC, set up an FTP connection to the device through the FTP client. Assume that the device IP address is 10.110.24.254.

```
C:\Documents and Setting\Administrator> ftp 10.110.24.254
Connected to 10.110.24.254.
220 FTP service ready.
User (10.110.24.254:(none)): huawei
331 Password required for huawei.
Password:
230 User logged in.
```

  c. Configure transfer parameters.

     If the FTP user is authenticated, the FTP client displays the prompt character of **ftp>**. Enter **binary** following the prompt character, and specify the path C:\temp where the uploaded file is to be saved on the FTP client.

```
ftp> binary
200 Type set to I.
ftp> lcd c:\temp
Local directory now C:\temp.
```

 Copyright © Huawei Technologies Co., Ltd.

d. Transfer the configuration file.

On the PC, run the **put** command to upload the configuration file to the specified path.

```
ftp> put backup.cfg
```

e. Check whether the **backup.cfg** file is successfully uploaded. If the **backup.cfg** file exists on the device and has the correct size, the configuration file recovery is successful.

f. Specify the recovered **backup.cfg** file as the configuration file for next startup.

```
<Huawei> startup saved-configuration backup.cfg
```

g. Restart the device. The configuration file recovery is complete.

```
<Huawei> reboot
Info: The system is comparing the configuration, please wait.
Warning: All the configuration will be saved to the next startup configuration. Continue? [y/n]: n
System will reboot! Continue? [y/n]: y
Info: system is rebooting ,please wait...
```

----End

12.3.5 Clearing the Configuration File

Context

You need to delete the configuration file when:

- The software and configuration file do not match after the device software is upgraded.
- The configuration file is damaged or an incorrect configuration file is loaded.

NOTICE

Exercise caution when you run the **reset saved-configuration** command. You are advised to run this command under the guide of technical support personnel.

Procedure

- Run the **reset saved-configuration** command to clear the next startup configuration file and cancel the configuration file used for next startup. The default device configurations are restored.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- If the current startup configuration file is the same as the next startup configuration file when you run the **reset saved-configuration** command, the current startup configuration file is also cleared.
- After you run this command and manually restart the device, the system displays a message asking you whether to save the configurations. Select N to clear the configurations.
- If you do not use the **startup saved-configuration** command to specify a new configuration file containing correct configurations or do not save the configuration file after running the **reset saved-configuration** command, the device uses factory configurations for startup. If the device does not have factory configurations, it uses default configurations for startup.
- If the next startup configuration file is empty, the device displays a message indicating that the file does not exist.

----End

12.3.6 Setting Factory Configurations

Context

You can configure basic information as factory configurations as needed. After the device is configured to restore factory configurations, you do not need to configure the basic information. If an unknown problem occurs on the device, or the device operations are slow or unstable after the device has been running for a long time, you can specify default factory settings as the factory configuration to restore the device to the initial state.

NOTICE

If you press and hold down the RESET button for at least 5 seconds, the device will restore to the latest factory settings after a restart. If the device needs to restore to the factory defaults, run the **set factory-configuration from default** command in the system view. It is recommended that you perform this operation under the guidance of technical support personnel.

Procedure

Step 1 Run **set factory-configuration from** { **current-configuration** | *filename* | **default** }

The current configuration, existing configuration file, or default factory configuration is configured as the factory configuration.

Step 2 (Optional) Run **set factory-configuration operate-mode** { **reserve-configuration** | **delete-configuration** | **delete-user-configuration** }

The mode of restoring the factory configuration is set to reserve or delete.

Reserve mode: The current configuration file will be reserved after you restore factory configurations.

Delete mode: The current configuration file will be deleted after you restore factory configurations.

 Copyright © Huawei Technologies Co., Ltd.

By default, the system reserves the previous configuration file when restoring the factory configuration.

NOTE

Only AR161EW, AR169EGW-L, AR2204XE-DC, and AR2204XE support **delete-user-configuration** parameter.

Step 3 (Optional) Run **factory-configuration reset**

The device is configured to restore the factory configuration after it restarts.

Step 4 Run **system-view**

The system view is displayed.

Step 5 (Optional) Run **change default-password**

The function of changing AAA and Boot passwords when factory settings of a device are restored is enabled.

To disable the function of changing AAA and Boot passwords when factory settings of a device are restored, run the **undo change default-password** command.

By default, the function of changing AAA and Boot passwords when factory settings of a device are restored is disabled. The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

NOTE

Only the AR169EW, AR169EGW-L, AR161EW, AR161EW-M1, AR2204XE, and AR2204XE-DC support this step.

Step 6 (Optional) Run **factory-configuration prohibit**

The command disables the function that restores the factory configurations of a device by holding down **RESET**.

If you want to restore the factory configurations of a device by holding down **RESET**, run the **undo factory-configuration prohibit** command to enable this function.

NOTE

Only the AR100&AR120&AR150&AR160&AR200 series support this command.

----End

Verifying the Configuration

- Run the **display factory-configuration** command to view the factory configuration information.
- Run the **display factory-configuration operate-mode** command to view the mode of restoring the factory configuration.

 Copyright © Huawei Technologies Co., Ltd.

12.4 Configuring System Startup Files

Pre-configuration Tasks

Specify the system software and configuration file for system startup so that the device will start and initialize with the specified software and configuration file. Specify new patch file if the system needs to load new patches.

Before configuring the system startup files, complete the following tasks:

- Start the device and logging in to the device locally or remotely.
- Save the system startup files in the root directory of the device.

NOTE

After downloading the system startup files from the server to the device, you can check whether the system startup files are damaged during the download process, for example, whether the files are completely downloaded. You can use a piece of third-party software (for example, HashMyFiles) on the server to calculate the MD5 or SHA256 value of the system software files, run the **display system** { **file-md5** | **file-sha256** } *filename* command on the device to calculate the MD5 or SHA256 value of the downloaded system software files, and compare the two values calculated on the server and device. If the two values are the same, the system startup files are not damaged. If the two values are different, the system startup files are damaged, and you need to download the files again.

Context

Before specifying the files for next startup, you can run the **display startup** command to view the specified files for next startup.

- If no system software is specified for next startup, the device will start with current system software. To change the system software to be loaded for next startup (during an upgrade for example), upload the new system software to the device and specify it as the system file for next startup. The system software package must use .cc as the file name extension and be saved to the root directory of the storage device. If the device has double SRUs, make sure that the system software is saved in the master SRU. When the system software is specified for the slave SRU, the device automatically copies the system software to the slave SRU.
- If no configuration file is specified for next startup, the device will start with the default configuration file (vrpcfg.zip for example). If no configuration file is stored in the default directory, the device uses the default parameters for initialization. The configuration file name extension must be .cfg or .zip. In addition, the configuration file must be saved to the root directory of the storage device.
- A patch file uses .pat as the file name extension. The specified patch file to be loaded for next startup must also be saved to the root directory of the storage device. If the device has double SRUs, make sure that the patch file is saved in the master SRU. When the patch file is specified for the slave SRU, the device automatically copies the patch file to the slave SRU.

NOTE

Only the AR3200 series supports dual SRUs.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

- Run **startup system-software** *filename* [**verify** | **signature** *sign-filename*]

  The system software to be loaded for next startup is specified.

  NOTE

  You cannot start the system software package in the system using an external hard disk.

  If the device has dual SRUs, run the **startup system-software** *filename* [**slave-board** | **all**] command to specify the system software for the slave SRU to load during the next startup.

  NOTE

  Specify the same system software for the master and slave SRUs.

  Specify the **verify** parameter to check the validity of the system software. If the verification fails, you cannot specify it as the system software to be loaded for next startup. This avoids startup failures caused by invalid system software.

  If **signature** *sign-filename* is specified, the device checks validity of the system software's digital signature file. If the check failed, the system software cannot be specified as the system software to be loaded for next startup. This configuration enhances device security.
- (Optional) Run **startup system-software** *filename* **backup**

  The backup system startup software is specified.

  When the startup software is damaged, the system uses the backup system software to start.

  By default, the device has no backup software system.
- (Optional) Run **startup system-software check enable**

  Security check over the system software package is enabled.

  By default, security check over the system software package is disabled.
- Run **startup saved-configuration** *configuration-file* [**slave-board** | **all**]

  The configuration file for next startup is specified.

  The device reads the configuration file from the root directory of the storage device for initialization when powered on.
- (Optional) Run **startup patch** *patch-name* [**slave-board** | **all**]

  The patch file for next startup is specified.

  To make the patch file take effect after the device restarts, run this command to specify the patch file for next startup.

----End

Verifying the Configuration

After the configuration is complete, run the **display startup** command to view the system software, backup system software, configuration file and patch file for next startup.

 Copyright © Huawei Technologies Co., Ltd.

12.5 Restarting the Device

Pre-configuration Tasks

Before restarting the device, complete the following tasks:

- Configure system startup files.

Context

Use one of the following methods to restart the device:

- Restart the device immediately after configuration: The device restarts immediately after the **reboot** command is run.
- Restart the device at scheduled time: The device can be restarted at a specified time later. When the configuration is complete, you can configure the device to restart at time when few services are running to minimize the impact of device restart on services.

The device restarts with the specified startup software. If the specified startup software is damaged, the device restarts with the backup startup software. If the restart still fails, the device searches the valid startup software package on the storage devices in the sequence "Flash memory-> SD card-> USB flash drive." If more than one valid startup software package is discovered, the device starts with the first discovered. When the device finds valid system software packages and configuration files on the storage device, it selects a rollback version and restarts with the selected version. If the device does not find valid system software and configuration file, it repeats the preceding operations.

NOTE

The AR100&AR120&AR150&AR160&AR200&AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204E-D-27GE, AR2204-24GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-48GE-P, AR2204E, AR2204E-D, AR2204-51GE, AR2204-51GE-R, AR2220L-DC, AR2220L-AC and AR3670 support the flash memory and USB flash drive. The AR2220-AC, AR2220-DC, AR2220E, AR2240C support the flash memory, hard disk and USB flash drive. The AR2204, AR2240 and AR3260 (using SRU40, SRU60, SRU80, SRU100, SRU100E, SRU200E, SRU200 and SRU400) support the flash memory, Micro SD card, and USB flash drive. The AR2240, AR2204XE-DC and AR2204XE support the Micro SD card and USB flash drive.

If the device starts using the system software package in the flash memory or SD card that contains a lot of fragmented files, the startup time is long. Delete unnecessary files in the flash memory or SD card.

NOTICE

- Do not restart the device unless necessary because device restart causes service interruption in a short time.
- Save the current configuration so that it will take effect after the device restarts.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

- Restart the device immediately.

  In the user view, run the **reboot** [**fast**] command to restart the device.

  - The **fast** parameter indicates quick restart of the device. The system does not ask you whether to save the configuration file in fast startup.
- Restart the device at scheduled time.

  In the user view, run the **schedule reboot** { **at** *time* | **delay** *interval* | **every** *time* } command to restart the device at scheduled time.

  - **at** *time* specifies the specific time to restart the device.
  - **delay** *interval* specifies the waiting time before restarting the device.

----End

Verifying the Configuration

- If scheduled restart is configured, run the **display schedule reboot** command to check the configuration of device restart.

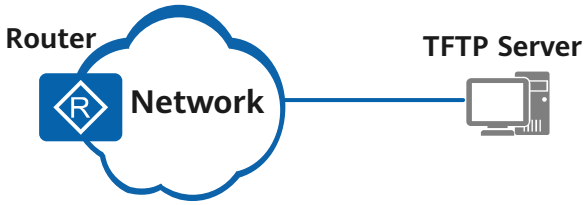
12.6 Configuration Examples for System Startup

12.6.1 Example for Backing Up the Configuration File

Networking Requirements

As shown in **Figure 12-2**, a user logs in to the device and backs up the configuration file to the TFTP server. So the configuration file can be recovered in case that the device is damaged.

Figure 12-2 Networking diagram of backing up the configuration file



Configuration Roadmap

The configuration roadmap is as follows:

1. Save the configuration file.
2. Back up the configuration file through TFTP.

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

Configuration file backup through TFTP is simple, but there are security risks. In scenarios with high security requirements, configuration file backup through SFTP is recommended. The following describes the configuration file backup process using TFTP as an example.

Procedure

Step 1 Save configurations to the **config.cfg** file.

```
<Huawei> save config.cfg
```

Step 2 Back up the configuration file through TFTP.

1. Start the TFTP server program.

   Start the TFTP server program on the PC. Set the path for transmitting the configuration file, and the IP address and port number of the TFTP server.

2. Transfer the configuration file.

   # Run the **tftp** command in the user view to back up the specified configuration file.

   ```
   <Huawei> tftp 10.110.24.254 put sd1:/config.cfg backup.cfg
   ```

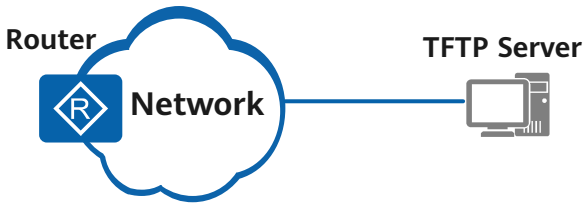
----End

12.6.2 Example for Recovering the Configuration File

Networking Requirements

As shown in **Figure 12-3**, a user logs in to the device and finds that some incorrect configurations cause errors in the system. To recover the original configuration, the user downloads the configuration file saved in the TFTP server to the device and specifies the configuration file for the next startup.

Figure 12-3 Network diagram of recovering the configuration file



Configuration Roadmap

The configuration roadmap is as follows:

1. Recover the configuration file that is backed up on the PC through TFTP.

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

Configuration file recovery through TFTP is simple, but there are security risks. In scenarios with high security requirements, configuration file recovery through SFTP is recommended. The following describes how to recover the configuration file that is backed up on a PC through TFTP.

2. Specify the recovered configuration file for the next startup.

Procedure

Step 1 Recover the configuration file that is backed up on the PC through TFTP.

1. Start the TFTP server program.

   Start the TFTP server program on the PC. Set the path for transmitting the configuration file, and the IP address and port number of the TFTP server.

2. Transfer the configuration file.

   # Run the **tftp** command in the user view.

   ```
   <Huawei> tftp 10.110.24.254 get backup.cfg config.cfg
   ```

Step 2 Specify the recovered configuration file for the next startup.

```
<Huawei> startup saved-configuration config.cfg
```

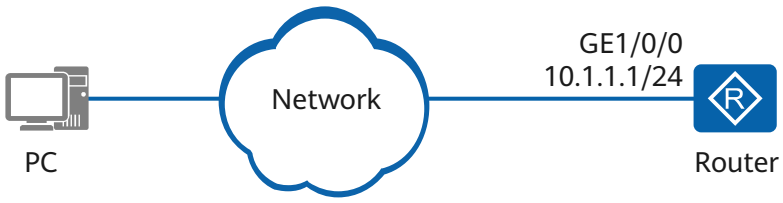
----End

12.6.3 Example of Configuring System Startup

Networking Requirements

As shown in **Figure 12-4**, the current system software cannot meet user needs. The device must load new software version with more features. Then the device software needs to be upgraded remotely.

Figure 12-4 Configuring System Startup Networking



Configuration Roadmap

The configuration roadmap is as follows:

1. Upload the new system software to the root directory of the device.
2. Save the current configuration so that it remains active after upgrade.
3. Specify the system software for next startup.

 Copyright © Huawei Technologies Co., Ltd.

4. Specify the configuration file for next startup of the device.
5. Restart the device to complete upgrade.

Procedure

Step 1 Upload the new system software to the root directory of the device.

Before configuration, run the **display startup** command to view the files for next startup.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] quit
<Router> display startup
MainBoard:
  Startup system software:                sd1:/basicsoft.cc
  Next startup system software:           sd1:/basicsoft.cc
  Backup system software for next startup:   null
  Startup saved-configuration file:       sd1:/vrpcfg.zip
  Next startup saved-configuration file:     sd1:/vrpcfg.zip
  Startup license file:                   null
  Next startup license file:                 null
  Startup patch package:                     null
  Next startup patch package:                null
  Startup voice-files:                    null
  Next startup voice-files:                  null
```

Upload the new system software to the device. This example uses FTP to transfer the system software. Configure the device as an FTP server and upload the system software to the device from the FTP client. Make sure there is enough space in the storage device before uploading files. If the space is insufficient, delete unnecessary files to free up space in the storage device.

```
<Router> system-view
[Router] ftp server enable
[Router] aaa
[Router-aaa] local-user huawei password irreversible-cipher Helloworld@6789
[Router-aaa] local-user huawei service-type ftp
[Router-aaa] local-user huawei ftp-directory sd1:
[Router-aaa] local-user huawei privilege level 15
[Router-aaa] quit
[Router] quit
```

Run the **ftp 10.1.1.1** command in the command line window of the PC to set up an FTP connection with the device. Run the **put** command to upload new system software **newbasicsoft.cc**. After the upload completes, run the **dir** command to check the system software.

```
<Router> dir
Directory of sd1:/

  Idx  Attr     Size(Byte)  Date        Time       FileName
    0  drw-              -  Apr 16 2012 13:19:58   logfile
    1  -rw-     85,925,409  Apr 16 2012 13:18:02   basicsoft.cc
    2  -rw-              4  Oct 27 2011 17:25:22   snmpnotilog.txt
    3  -rw-          6,033  Jul 16 2012 16:40:02   private-data.txt
    4  -rw-          3,275  Jul 14 2012 14:18:08   vrpcfg.zip
    5  drw-              -  Nov 14 2011 19:14:26   sysdrv
    6  drw-     88,239,759  Jul 16 2012 19:14:26   newbasicsoft.cc
...

1,927,220 KB total (1,130,464 KB free)
```

Step 2 Save the current configuration to the default storage device.

 Copyright © Huawei Technologies Co., Ltd.

```
<Router> save
The current configuration will be written to the device.
Are you sure to continue? [Y/N]y
Now saving the current configuration to the slot 0 .
Info: Save the configuration successfully.
```

Step 3 Specify the system software to be loaded for next startup.

```
<Router> startup system-software newbasicsoft.cc
```

Step 4 Specify the configuration file for next startup.

```
<Router> startup saved-configuration vrpcfg.zip
```

NOTE

In step 1, you can run the **display startup** command to check the configuration file for next startup. The message "Next startup saved-configuration file: sd1:/**vrpcfg.zip**" will be displayed. This means the **vrpcfg.zip** configuration file has been specified for next startup, so you do not need to perform this step. To specify another file for next startup, perform this step.

Step 5 Verify the configuration.

Run the following command to view the system software and configuration file for next startup.

```
<Router> display startup
MainBoard:
  Startup system software:                sd1:/basicsoft.cc
  Next startup system software:           sd1:/newbasicsoft.cc
  Backup system software for next startup:   null
  Startup saved-configuration file:       sd1:/vrpcfg.zip
  Next startup saved-configuration file:     sd1:/vrpcfg.zip
  Startup license file:                   null
  Next startup license file:              null
  Startup patch package:                  null
  Next startup patch package:             null
  Startup voice-files:                    null
  Next startup voice-files:               null
```

Step 6 Restart the device.

Since the configuration file has been saved, run the **reboot fast** command to restart the device quickly.

```
<Router> reboot fast
System will reboot! Continue? [Y/N]:y
Info: system is rebooting ,please wait...
```

Step 7 Verify the configuration.

Wait for several minutes until the device restart is complete. Run the **display version** command to check the current system version. If the current system software is new, the upgrading has succeeded.

The **display version** command output is not provided here.

----End

Configuration File

```
#
aaa
 local-user huawei password irreversible-cipher %^%#,))E=[pEbYRK$p4\_no/Mjz3#bSXH4+'!So.E/(xr}|+jz6M
%^%#
 local-user huawei privilege level 15
 local-user huawei ftp-directory sd1:
```

 Copyright © Huawei Technologies Co., Ltd.

```
 local-user huawei service-type ftp
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
#
 ftp server enable
#
return
```

13 BootROM Menu

About This Chapter

BootROM provides the configuration restoration and software upgrade functions to ensure device security and implement basic device maintenance.

NOTE

BootROM screen is just for reference.

13.1 Overview of the BootROM Menu

13.2 Licensing Requirements and Limitations for the BootROM Menu
This section provides the configuration precautions of BootROM menu introduction.

13.3 BootROM Main Menu

13.4 Serial Menu

13.5 Network Menu

13.6 Startup Select

13.7 File Manager

13.8 Password Manager

13.9 FAQ About the BootROM Menu
This section describes common problems that may occur during the configuration and their solutions.

13.1 Overview of the BootROM Menu

The boot read-only memory (BootROM) is a firmware stored in the read-only memory (ROM) chip of the device main board. The BootROM contains basic input/output programs, system settings, power on self-test (POST) programs, and system automatic startup program.

You can use the BootROM menu to perform the following operations:

 Copyright © Huawei Technologies Co., Ltd.

- Restore or upgrade the system when the system stops responding and the command line interface (CLI) cannot be displayed.
- Back up the configuration file to prevent configuration loss.
- Change the password for accessing the BootROM menu, preventing unauthorized users from accessing the BootROM menu.
- Access this menu to log in to the device using the console port without entering the password when you forget the password.

13.2 Licensing Requirements and Limitations for the BootROM Menu

This section provides the configuration precautions of BootROM menu introduction.

Involved Network Elements

None

Licensing Requirements

BootROM menu introduction is a basic feature of a router and is not under license control.

Feature Limitations

If the device has two main control boards installed, when clearing the console port password through the BootROM, clear the password of the active main control board, and then install the standby main control board.

13.3 BootROM Main Menu

You have logged in to the device using the console port.

NOTE

For details about how to log in to the device using the console port, see **9.4.4 Logging In to a Device Through the Console Port**. To use third-party terminal emulation software, set the communication parameters correctly. If the parameter settings are incorrect, the third-party software may enter excess characters, leading to abnormal BIOS menu functions.

Restart the device. Press Ctrl+B in 3 seconds to enter the BootROM main menu when the following message is displayed.

```
Press Ctrl+B to break auto startup ... 3

Enter Password:******


    Main Menu

  1. Default Startup
  2. Serial Menu
  3. Network Menu
```

 Copyright © Huawei Technologies Co., Ltd.

```
  4. Startup Select
  5. File Manager
  6. Reboot
  7. Password Manager

Enter your choice(1-7):
```

The AR100&AR120&AR150&AR160&AR200&AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204E-D-27GE, AR2204-24GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-48GE-P, AR2204E, AR2204E-D, AR2204-51GE, AR2204-51GE-R, AR2220L-DC, AR2220L-AC and AR3670 support the flash memory and USB flash drive. The AR2220-AC, AR2220-DC, AR2220E, AR2240C support the flash memory, hard disk and USB flash drive. The AR2204, AR2240 and AR3260 (using SRU40, SRU60, SRU80, SRU100, SRU100E, SRU200E, SRU200 and SRU400) support the flash memory, Micro SD card, and USB flash drive. The AR2240, AR2204XE-DC and AR2204XE support the Micro SD card and USB flash drive.

In this chapter, the micro SD card is used as a storage device.

NOTE

The display menus vary according to the device model.

Table 13-1 BootROM main menu

Item	Description
Press Ctrl+B to break auto startup	Press **Ctrl+B** in 3 seconds to access the BootROM menu. You can access the BootROM menu for debugging after failing to access the CLI on the device. To set the startup waiting time, select **5. Set Startup Waiting Time** in **4. Startup Select**. The default time is 3 seconds.
Enter Password	Enter the password for accessing the BootROM menu. The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it. If you enter incorrect passwords for three consecutive times, the system restarts. To change the password, select **1. Modify the menu password** in **7. Password Manager**. You are advised to change the password in a timely manner and update the password periodically after login to ensure device security.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
1. Default Startup	Select this item to quickly start the device. When the modified parameters do not affect system initialization before the BootROM menu is displayed, select **1. Default Startup** to start the device to avoid duplicate initialization. This operation does not restart the BootROM, but continues to start the system. If the device does not have **Default Startup**, you can select **Reboot**.
2. Serial Menu	Access the serial interface submenu to update the BootROM and complex programmable logical device (CPLD). This operation can be performed after a PC is connected to the device using the serial interface, without other configuration. However, the file transfer speed is low. **NOTE** You are advised to update the BootROM and CPLD with the instructions of technical support personnel.
3. Network Menu	Access the network interface submenu to obtain files from the management interface. The file transfer speed is high. You need to set network parameters and configure the file server to ensure a reachable route between the device and the file server.
4. Startup Select	Access the startup submenu to view or modify startup configuration.
5. File Manager	Access the file system submenu to manage and maintain the file system.
6. Reboot	When the modified parameters affect system initialization before the BootROM menu is displayed, select **6. Reboot** to restart the BootROM and then start the system.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
7. Password Manager	Access this menu to change the password for accessing the BootROM menu, preventing unauthorized users from accessing the BootROM menu. Access this menu to log in to the device using the console port without entering the password when you forget the password.
Shortcut key	The BootROM menu provides two shortcut keys: Ctrl+M, Ctrl+J. The two shortcut keys can be used in any BootROM menu to provide functions similar to **Enter**.

Displaying/hiding the Boot menu

NOTE

Only the AR161EGW-LM1, AR161EW, AR161EW-M1, AR169E, AR169EGW-L, AR169EW, AR2204XE and AR2204XE-DC support this function.

- In the system view, run **bootloader startup menu enable**
  Display the Boot menu.
- In the system view, run **display bootloader startup menu**
  Check whether the Boot menu is hidden.

13.4 Serial Menu

Access the BootROM main menu and select **2** to access the serial interface submenu.

```
      Main Menu

  1. Default Startup
  2. Serial Menu
  3. Network Menu
  4. Startup Select
  5. File Manager
  6. Reboot
  7. Password Manager

Enter your choice(1-7):2

      Serial Menu

  1. Update Bootrom
  2. Update CPLD Chip 0
  3. Modify baud rate
  0. Return

Enter your choice(0-3):
```

The AR161&AR161W&AR161G-L&AR161G-Lc&AR161EW&AR161EW-M1&AR169&AR169W&AR169G-L&AR169EGW-L&AR169-P-M9&AR169W-P-

 Copyright © Huawei Technologies Co., Ltd.

M9&AR169RW-P-M9&AR120&AR100 series routers do not support the submenus **Update Bootrom** and **Update CPLD Chip 0**.

Table 13-2 Serial interface submenu

Item	Description
1. Update Bootrom	Update the BootROM through the serial interface.
2. Update CPLD Chip 0	Update the CPLD through the serial interface.
3. Modify baud rate	Modify parameters of the serial interface. The default transmission rate is 9600 bit/s. The serial interface supports the following transmission rates: ● 9600 bit/s ● 19200 bit/s ● 38400 bit/s ● 57600 bit/s ● 115200 bit/s After the transmission rate on the serial interface is modified, synchronize the transmission rate on the PC to that on the serial interface and reconnect the PC to the device.
0. Return	Return to the main menu.

13.5 Network Menu

Access the BootROM main menu and select **3** to access the network interface menu.

```
      Main Menu

  1. Default Startup
  2. Serial Menu
  3. Network Menu
  4. Startup Select
  5. File Manager
  6. Reboot
  7. Password Manager

Enter your choice(1-7):3
      Network Menu

  1. Display parameter
  2. Modify parameter
  3. Save parameter
  4. Download file
  5. Upload file
  0. Return

Enter your choice(0-5):
```

 Copyright © Huawei Technologies Co., Ltd.

Table 13-3 Network interface Menu

Item	Description
1. Display parameter	Display network parameters.
2. Modify parameter	Set network interface menu parameters before downloading or uploading files. The network parameter settings take effect only in this startup process.
3. Save parameter	Save network parameter settings. The saved network parameter settings still take effect after the system restarts.
4. Download file	Download files from the server to the device. If incorrect configurations result in abnormal functions, you can restore the configuration and patch files in the storage device using this menu. **NOTE** If the AR2240 or AR3260 is equipped with the SRU200, SRU200E, and an exception occurs on the network when the device is downloading a file from the server, the file transmission is interrupted. After the network recovers, the device automatically deletes the file whose transmission is interrupted and downloads the file again.
5. Upload file	Uploads files from the device to the server. To prevent configuration information loss, back up the configuration and patch files in the storage device using this menu.
0. Return	Return to the BootLoader main menu.

13.5.1 Modify parameter

Access the network interface submenu and select **2** to access the modify parameter menu.

```
      Network Menu

  1. Display parameter
  2. Modify parameter
  3. Save parameter
  4. Download file
  5. Upload file
  0. Return

Enter your choice(0-5):2
NOTE:
Net type define:  0(ftp), 1(tftp),
ENTER = no change; '.' = clear;

Net type           : 0
File name          : cfg.zip
Ethernet ip address : 192.168.1.3
```

 Copyright © Huawei Technologies Co., Ltd.

```
Ethernet ip mask    : ffffff00
Gateway ip address  :
Ftp host ip address : 192.168.1.11
Ftp user            : huawei
Ftp password        : **********

Modify net parameter success.
```

- Start the TFTP or FTP software on the PC. (For details, see help document about the third-party software.)

  NOTE

  Use this menu to set network interface parameters in FTP or TFTP mode. The PC must function as the FTP or TFTP server. Ensure that the PC is directly connected to the management interface of the device and can communicate on the same network segment.

- Set network interface parameters.

  The parameter values can contain only letters, numerals, underlines, and dots. Spaces are not allowed.

  - **Net type**: FTP client or TFTP client. By default, the device functions as the FTP client.
  - **File name**: Name of the file to be transferred.
  - **Ethernet ip address**: IP address of the management interface on the device. By default, the IP address of the management interface is 192.168.1.20.
  - **Ethernet ip mask**: Subnet mask.
  - **Gateway ip address**: Gateway IP address.
  - **Ftp host ip address**: TFTP or FTP server IP address.
  - **Ftp user**: Name of the user who connects to the FTP server.
  - **Ftp password**: Password for accessing the FTP server.

  NOTE

  When the device transfers files using TFTP, the **Ftp user** and **Ftp password** parameters is not required. You only need to press **Enter**.

  If the device and server belong to different network segments, the **Gateway ip address** parameter must be set. If the device and server belong to the same network segment, the **Gateway ip address** parameter is not required.

13.6 Startup Select

Access the BootROM main menu and select **4** to access the startup select menu.

```
      Main Menu

  1. Default Startup
  2. Serial Menu
  3. Network Menu
  4. Startup Select
  5. File Manager
  6. Reboot
  7. Password Manager

Enter your choice(1-7):4
      Startup Select
```

```
  1. Display Startup
  2. Set Boot File
  3. Set Config File
  4. Startupfile Check Manage
  5. Set Startup Waiting Time
  0. return

Enter your choice(0-5):
```

Table 13-4 Startup select menu

Item	Description
1. Display Startup	Display the system software and configuration file used in the current and last startup. Before upgrading or degrading the system, check whether the system software and configuration file are correct using this menu.
2. Set Boot File	Specify the system software for next startup. Before upgrading or degrading the system, specify the system software for the next startup using this menu.
3. Set Config File	Specify the configuration file for the next startup. Before upgrading or degrading the system, specify the configuration file for the next startup using this menu.
4. Startupfile Check Manage	Manage startup file check. To view or modify startup file check configurations, manage startup file check using this menu.
5. Set Startup Waiting Time	Set the start waiting time. You need to enter the startup waiting time that ranges from 3 to 9, in seconds. The default time is 3 seconds. The changed startup waiting time takes effect only in this startup process. When the system restarts, the startup waiting time restores to 3 seconds.
0. return	Return to the BootLoader menu.

13.6.1 Display Startup

Access the startup select submenu and select **1** to access the display startup menu.

```
    Startup Select

  1. Display Startup
  2. Set Boot File
```

 Copyright © Huawei Technologies Co., Ltd.

```
   3. Set Config File
   4. Startupfile Check Manage
   5. Set Startup Waiting Time
   0. return

Enter your choice(0-5):1

************** Current Stratup info ****************
Valid Flag State       : Vaild
Boot File Name         : sd1:/softwarenew.cc
Config File Name       : sd1:/cfgnew.zip
Licence File Name      :
Patch File Name        :
Voice File Name        :


************** Pre Startup info ********************
Valid Flag State       : Vaild
Boot File Name         : sd1:/software.cc
Config File Name       : sd1:/cfg.zip
Licence File Name      :
Patch File Name        : sd1:/patch.pat
Voice File Name        :
```

Displays files used in the current and last startup, such as the system software and configuration file.

13.6.2 Set Boot File

Access the startup select submenu and select **2** to access the set boot file menu.

Before upgrading or degrading the system, specify the system software used for startup using this menu.

Select the serial number of the storage device where the system software locates. The storage device can be the flash memory, micro SD card, or USB disk.

```
      Startup Select

   1. Display Startup
   2. Set Boot File
   3. Set Config File
   4. Startupfile Check Manage
   5. Set Startup Waiting Time
   0. return

Enter your choice(0-5):2
      Select Boot File

   1. Flash
   2. SDCard[1]
   0. Return

Enter your choice(0-2):2
NOTE: Boot file must be .cc or .CC

Current boot file: sd1:/softwarenew.cc
Press ENTER directly for no change.
Or, please input the new file name: sd1:/softwarenew1.cc
Save the boot file name: sd1:/softwarenew1.cc ? Yes or No(Y/N)y
Save load state word...OK!
```

For the AR161&AR161W&AR161EW&AR161EW-M1&AR161G-L&AR161G-Lc&AR169&AR169G-L&AR169EGW-L&AR169-P-M9&AR169W-P-M9&AR1220V&AR1220W&AR1220VW&AR1220E&AR1220EV&AR1220EVW&AR1220C&AR2204-51GE-P&AR2204-51GE&AR2204-51GE-R&AR2204-27GE-

 Copyright © Huawei Technologies Co., Ltd.

P&AR2204-27GE&AR2204E-D-27GE&AR2204E&AR2204E-D, if the check flag for the digital signature file of the system software is set based on **13.6.4 Startupfile Check Manage**, the procedure for specifying the startup system software is as follows:

```
      Startup Select

  1. Display Startup
  2. Set Boot File
  3. Set Config File
  4. Startupfile Check Manage
  5. Set Startup Waiting Time
  0. return

Enter your choice(0-5):2
      Select Boot File

  1. flash
  0. Return

Enter your choice(0-1):1
NOTE: Boot file must be .cc or .CC

Current boot file: flash:/software.cc
Press ENTER directly for no change.
Or, please input the new file name: flash:/softwarenew.cc
      Signature file Select

  0. Flash

Enter your choice(0-0): 0
Input the signature file: flash:/softwarenew.cc.asc
 Verifying,This may last a few minutes.Please Wait......
 Step1: Pre-deal with keyfile in start packet ...OK
 Step2: Pre-deal with applied signature file ...OK
 Step3: Pre-deal with target boot file ...OK
 Step4: Verifying Data.....OK
 signature file check success!

Signature check success!
Save the boot file name: falsh:/softwarenew.cc ? Yes or No(Y/N) Y
Save load state word...OK!
```

13.6.3 Set Config File

Access the startup select submenu and select **3** to access the set config file menu.

```
      Startup Select

  1. Display Startup
  2. Set Boot File
  3. Set Config File
  4. Startupfile Check Manage
  5. Set Startup Waiting Time
  0. return

Enter your choice(0-5):3
      Select Config File

  1. Flash
  2. SDCard[1]
  0. Return

Enter your choice(0-2):2
NOTE: Config file must be .zip or .cfg or .ZIP or .CFG

Current Config file: sd1:/cfgnew.zip
```

 Copyright © Huawei Technologies Co., Ltd.

```
Press ENTER directly for no change.
Or, please input the new file name: sd1:/cfgnew1.zip
Save the config file name: sd1:/cfgnew1.zip ? Yes or No(Y/N)y
Save load state word...OK!
```

To specify the configuration file for startup based on users' requirements, use this menu.

Select the serial number of the storage device where the configuration file locates. The storage device can be the flash memory, micro SD card, or USB disk.

13.6.4 Startupfile Check Manage

Access the startup select submenu and select **4** to access the startup file check manage menu.

To view or modify startup file check configurations, manages startup file check using this menu.

```
      Startup Select

  1. Display Startup
  2. Set Boot File
  3. Set Config File
  4. Startupfile Check Manage
  5. Set Startup Waiting Time
  0. return

Enter your choice(0-5):4
      File Check Manage

  1. Set FileCheck Flag
  2. Clear FileCheck Flag
  3. Query FileCheck Flag
  4. Set SignatureCheck Flag
  5. Clear SignatureCheck Flag
  6. Query SignatureCheck Flag
  0. return

Enter your choice(0-6):1
STUP_SetFileCheckFlag Success!

      File Check Manage

  1. Set FileCheck Flag
  2. Clear FileCheck Flag
  3. Query FileCheck Flag
  4. Set SignatureCheck Flag
  5. Clear SignatureCheck Flag
  6. Query SignatureCheck Flag
  0. return

Enter your choice(0-6):3
StartUp FileCheck Flag Exist

      File Check Manage

  1. Set FileCheck Flag
  2. Clear FileCheck Flag
  3. Query FileCheck Flag
  4. Set SignatureCheck Flag
  5. Clear SignatureCheck Flag
  6. Query SignatureCheck Flag
  0. return

Enter your choice(0-6):2
```

 Copyright © Huawei Technologies Co., Ltd.

```
STUP_ClearFileCheckFlag Success!

      File Check Manage

   1. Set FileCheck Flag
   2. Clear FileCheck Flag
   3. Query FileCheck Flag
   4. Set SignatureCheck Flag
   5. Clear SignatureCheck Flag
   6. Query SignatureCheck Flag
   0. return

Enter your choice(0-6):3
StartUp FileCheck Flag not Exist

      File Check Manage

   1. Set FileCheck Flag
   2. Clear FileCheck Flag
   3. Query FileCheck Flag
   4. Set SignatureCheck Flag
   5. Clear SignatureCheck Flag
   6. Query SignatureCheck Flag
   0. return

Enter your choice(0-6):4
Set SignatureCheckFlag Success!

      File Check Manage

   1. Set FileCheck Flag
   2. Clear FileCheck Flag
   3. Query FileCheck Flag
   4. Set SignatureCheck Flag
   5. Clear SignatureCheck Flag
   6. Query SignatureCheck Flag
   0. return

Enter your choice(0-6):6
StartUp SignatureCheck Flag Exist

      File Check Manage

   1. Set FileCheck Flag
   2. Clear FileCheck Flag
   3. Query FileCheck Flag
   4. Set SignatureCheck Flag
   5. Clear SignatureCheck Flag
   6. Query SignatureCheck Flag
   0. return

Enter your choice(0-6):5
Clear SignatureCheckFlag Success!

      File Check Manage

   1. Set FileCheck Flag
   2. Clear FileCheck Flag
   3. Query FileCheck Flag
   4. Set SignatureCheck Flag
   5. Clear SignatureCheck Flag
   6. Query SignatureCheck Flag
   0. return

Enter your choice(0-6):6
StartUp SignatureCheck Flag not Exist
```

Table 13-5 Startupfile Check Manage

Item	Description
1. Set FileCheck Flag	Set the check flag for the system software. The check flag is used for performing the system software check.
2. Clear FileCheck Flag	Cancel the check flag for the system software.
3. Query FileCheck Flag	Check whether the check flag for the system software is set.
4. Set SignatureCheck Flag	Set the check flag for the digital signature file of the system software. The check flag is used for performing the validity check for the digital signature file of the system software.
5. Clear SignatureCheck Flag	Cancel the check flag for the digital signature file of the system software.
6. Query SignatureCheck Flag	Check whether the check flag for the digital signature file of the system software is set.
0. Return	Return to the main menu.

Only the AR161&AR161W&AR161EW&AR161EW-M1&AR161G-L&AR161G-Lc&AR169&AR169G-L&AR169EGW-L&AR169-P-M9&AR169W-P-M9&AR1220V&AR1220W&AR1220VW&AR1220E&AR1220EV&AR1220EVW&AR1220C&AR2204-51GE-P&AR2204-51GE&AR2204-51GE-R&AR2204-27GE-P&AR2204-27GE&AR2204E-D-27GE&AR2204E&AR2204E-D support items 4, 5, and 6 in the menu.

13.7 File Manager

Access the BootROM main menu and select **5** to access the file manager menu.

```
      Main Menu

  1. Default Startup
  2. Serial Menu
  3. Network Menu
  4. Startup Select
  5. File Manager
  6. Reboot
  7. Password Manager

Enter your choice(1-7):5
      File Menu

  1. Flash file system
  2. SDCard file system
  0. Return

Enter your choice(0-2):
```

- Access the main menu and select **1** to access the flash file system menu.

  ```
      File Menu
  ```

```
  1. Flash file system
  2. SDCard file system
  0. Return

Enter your choice(0-2):1
      Flash file system MENU

  1. List file in flash
  2. Delete file in flash
  3. Rename file in flash
  4. Format Flash file system
  5. Check Flash file system
  0. Return

Enter your choice(0-5):0
```

NOTE

The **Check Flash file system** item is added to the menu only for the AR150&AR160&AR200&AR2200 series.

- Access the main menu and select **2** to access the SD card file system menu.

```
      File Menu

  1. Flash file system
  2. SDCard file system
  0. Return

Enter your choice(0-2):2
      SDCard file system MENU

  1. List file in SDCard[1]
  2. Delete file in SDCard[1]
  3. Rename file in SDCard[1]
  4. Format SDCard[1]
  5. Check SDCard[1]
  0. Return

Enter your choice(0-5):
```

  - Select **1** to access the List file in SDCard[1] menu.

```
Enter your choice(0-5):1
Files of the device:

drwxrwxrwx         -  Dec 27 2012 07:07:00   logfile
-rwxrwxrwx  77773440  Dec 16 2011 15:18:08   software.cc
-rwxrwxrwx 103661312  Nov 27 2012 19:46:48   softwarenew.cc
-rwxrwxrwx      1241  Mar 03 2012 17:30:34   rootcert.pem
-rwxrwxrwx  86307328  Apr 27 2012 15:11:36   softwarenew1.cc
-rwxrwxrwx      1728  Apr 27 2012 19:21:38   patch.dat
-rwxrwxrwx      3275  Dec 16 2012 07:50:50   cfg.zip
-rwxrwxrwx      2172  Dec 16 2012 14:18:08   cfgnew.zip
-rwxrwxrwx      5414  Dec 17 2012 19:14:26   cfgnew1.zip
-rwxrwxrwx    558320  Sep 18 2012 20:04:10   test.txt
10 files found!
1973735424 Byte total, 1031127040 Byte free.
```

  - Select **2** to access the Delete file in SDCard[1] menu.

```
Enter your choice(0-5):2
BE CAREFUL!
This may cause your system fail to start!
Please input the file name you want to delete: test.txt
delete it? Yes or No(Y/N): y
Deleting file[sd1:/test.txt], please wait....Done
```

  - Select **3** to access the Rename file in SDCard[1] menu.

```
Enter your choice(0-5):3
Please input the file name: cfg.zip
Please input the new name: vrpcfg.zip
```

```
Rename file[sd1:/cfg.zip] to [sd1:/vrpcfg.zip], Yes or No(Y/N): y
Rename OK!
```

- Select **4** to access the Format SDCard[1] menu.

NOTICE

After the storage device is formatted, all data including historical system software and configuration files are lost. Therefore, use this menu with caution.

```
Enter your choice(0-5):4
BE CAREFUL!
All files in the device will be lost.
This may cause your system fail to start!
Are you sure to format it? Yes or No(Y/N): y
Format file system. Please wait....

Format success!
```

- Select **5** to access the Check SDCard[1] menu.

```
Enter your choice(0-5):5
Check SD Card[1] file system. Please wait....

          sd1:/  - Volume is OK

File system check OK!
```

Table 13-6 File system submenu

Item	Description
1. List file in flash/SDCard[1]	Display all files in the flash memory or the micro SD card.
2. Delete file in flash/ SDCard[1]	Delete files in the flash memory or the micro SD card.
3. Rename file in flash/ SDCard[1]	Rename directories or files in the flash memory or the micro SD card.
4. Format flash/SDCard[1]	Format the flash memory or the micro SD card.
5. Check flash/SDCard[1]	Check the validity of the flash memory or the micro SD card.
0. Return	Return to the BootLoader main menu.

13.8 Password Manager

Access the BootROM main menu and select **7** to access the password manager menu.

```
    Main Menu

  1. Default Startup
  2. Serial Menu
```

 Copyright © Huawei Technologies Co., Ltd.

```
  3. Network Menu
  4. Startup Select
  5. File Manager
  6. Reboot
  7. Password Manager

Enter your choice(1-7):7
      PassWord Menu

  1. Modify the menu password
  2. Clear the console login password
  0. Return

Enter your choice(0-2):1
Modify password. Press Ctrl+c to break.
  //On AR161&AR161G-LE&AR169&AR169G-LE&AR169-P-M9&AR169W-P-M9&AR169RW-P-M9 and AR120
series&AR100 series, the following information is displayed: Modify password. the password length must >=
6.Press Ctrl+c to break.

Enter Old Password:******
Input new password:******
Input new password again:******
Are you sure to change password? [y/n]:y
Save new password Success.

      PassWord Menu

  1. Modify the menu password
  2. Clear the console login password
  0. Return

Enter your choice(0-2):2
Clear the console login password Succeed!
```

To prevent unauthorized users from accessing the BootROM main menu, select **Modify the menu password** to change the password for access the BootROM main menu.

When you forget the password for login using the console interface, select **Clear the console login password** to clear the login password.

13.9 FAQ About the BootROM Menu

This section describes common problems that may occur during the configuration and their solutions.

13.9.1 How Do I Log in to the Device Using BootROM If I Forget the Console Login Password

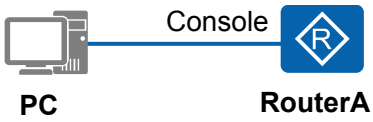
The console interface on RouterA connects to the PC and the console login password is forgotten. It is required that BootROM be used to log in to the device. This example applies to V200R003C00 and later versions, and all AR models.

NOTE

If the device has two main control boards installed, you need to remove the standby main control board before performing the following operations, and then install it after the following operations are complete.

 Copyright © Huawei Technologies Co., Ltd.

Figure 13-1 Networking for login through BootROM when the console login password is forgotten



1. Log in to the router through the console port.

   NOTE

   When performing operations, ensure that users on the serial port are kept online.

2. Restart RouterA. Press **Ctrl+B** to enter the BootROM menu when the following information is displayed:

```
BIOS Creation Date : Nov 10 2011, 14:41:12
DDR DRAM init : OK
Start Memory Test ? ('t' or 'T' is test):skip
Copying Data : Done
Uncompressing : Done
USB2 Host Stack Initialized.
USB Hub Driver Initialized
USBD  Wind River Systems, Inc. 562 Initialized
Octeon Host Controller Initialize.....Done.


Press Ctrl+B to break auto startup ... 3
```

   NOTE

   After pressing **Ctrl+B**, you need to enter the password to enter the BootROM menu. The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

3. Select choice 7 to enter the Password Manager menu.

```
    Main Menu

  1. Default Startup
  2. Serial Menu
  3. Network Menu
  4. Startup Select
  5. File Manager
  6. Reboot
  7. Password Manager

Enter your choice(1-6):7
```

4. Select choice 2 to delete the console login password.

```
    PassWord Menu

  1. Modify the menu password
  2. Clear the console login password
  0. Return

Enter your choice(0-1):2
Clear the console login password Succeed!

    PassWord Menu

  1. Modify the menu password
  2. Clear the console login password
  0. Return
```

 Copyright © Huawei Technologies Co., Ltd.

```
Enter your choice(0-1):0
```

5. Select 1 and wait for a while. Then you can log in to the device.

   NOTE

   Configuring the authentication mode and password for the console user interface is necessary; otherwise, after the device is restarted, users still need to be authenticated using the original password when they log in to the device through the console port.

```
  Main Menu

1. Default Startup
2. Serial Menu
3. Network Menu
4. Startup Select
5. File Manager
6. Reboot
7. Password Manager

Enter your choice(1-6):1
```

14 BootLoader Menu on the AR3600

About This Chapter

The BootLoader menu on the AR3600 provides system software upgrade and console port password deletion. When the AR3600 becomes faulty and the command line interface cannot be accessed, you can use the BootLoader menu to restore the device status.

14.1 Overview of the BootLoader Menu

14.2 Licensing Requirements and Limitations for the BootLoader Menu
This section provides the configuration precautions of BootLoader menu introduction.

14.3 BootLoader Menu

14.4 Serial SubMenu

14.5 Ethernet SubMenu

14.6 Modify Startup Parameters

14.7 File System

14.8 Password Manager

14.9 Configuration Examples for the BootLoader Menu on the AR3600

14.1 Overview of the BootLoader Menu

On the AR3600, the BootLoader is a Linux application and is used to upgrade system files, save system settings, and manage files in partitions and startup programs.

You can use the BootLoader menu in the following situations:

- When the system breaks down and the command line interface cannot be accessed, use the BootLoader menu to restore or upgrade the system.

 Copyright © Huawei Technologies Co., Ltd.

- To prevent configuration loss, use the BootLoader menu to back up the configuration file.
- To prevent unauthorized users from accessing the BootLoader menu, use the BootLoader menu to modify the password for accessing the BootLoader menu.
- When you fail to log in to the device because the console port password is forgotten, use the BootLoader menu to delete the console port password.

14.2 Licensing Requirements and Limitations for the BootLoader Menu

This section provides the configuration precautions of BootLoader menu introduction.

Involved Network Elements

None

Licensing Requirements

The BootLoader menu is a basic feature of a router and is not under license control.

Feature Limitations

None

14.3 BootLoader Menu

Log in to the device through the console port.

NOTE

For details on how to connect the console port to the device, see **9.4.4 Logging In to a Device Through the Console Port**. If third-party terminal simulation software is used, set communication parameters. If parameter settings are incorrect, the third-party software may input additional characters when you perform operations through the BIOS menu. As a result, some operations may fail to be performed.

Restart the device. When the system displays the following information, press **Ctrl +B** within 3s to access the BootLoader menu.

```
Press Ctrl+B to break auto startup ... 3

Enter Password:******


    BootLoader Menu

  1. Default Startup
  2. Serial SubMenu
  3. Ethernet SubMenu
  4. Modify Startup Parameters
  5. File System
```

 Copyright © Huawei Technologies Co., Ltd.

```
  6. Password Manager
  7. Reboot

Enter your choice(1-7):
```

The AR3600 supports the flash memory and USB flash drive.

Here, the flash memory is used as an example.

Table 14-1 BootLoader menu

Item	Description
Press Ctrl+B to break auto startup	Press **Ctrl+B** within 3s to access the BootLoader menu. Generally, when the command line interface cannot be accessed, access the BootLoader menu to debug the device.
Enter Password	Enter the password. The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it. If you enter the incorrect password for three consecutive times, the system restarts. You can modify the password through **1. Modify bootloader Password** in **6. Password Manager**.
1. Default Startup	To rapidly start the device, perform this operation. When the modified parameters do not affect the initialization of the BootLoader menu, start the device through **1. Default Startup** to prevent the device from being initialized repeatedly. After this operation is performed, the device starts up from the current phase.
2. Serial SubMenu	To set the baud rate of the serial port, access this menu.
3. Ethernet SubMenu	To obtain files through the management port, access this menu. The file transfer speed is fast, but you need to set network parameters and configure the file server to ensure that there is a reachable route between the device and file server.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
4. Modify Startup Parameters	To view and modify the startup configuration, access this menu.
5. File System	To manage and maintain the file system, access this menu.
6. Password Manager	To prevent unauthorized users from accessing the BootLoader menu, access this menu to modify the password for accessing the BootLoader menu. When you fail to log in to the device because the console port password is forgotten, access this menu to delete the console port password.
7. Reboot	When the modified parameters affect the initialization of the BootLoader menu, access this menu to restart the BootLoader. Then start the device.

14.4 Serial SubMenu

Access the BootLoader menu and select **2** to access the **Serial SubMenu**.

```
    BootLoader Menu

  1. Default Startup
  2. Serial SubMenu
  3. Ethernet SubMenu
  4. Modify Startup Parameters
  5. File System
  6. Password Manager
  7. Reboot

Enter your choice(1-7):2

    Serial SubMenu

  1. Modify baud rate
  0. Return

Enter your choice(0-1):
```

 Copyright © Huawei Technologies Co., Ltd.

Table 14-2 Serial SubMenu

Item	Description
1. Modify baud rate	Change the parameters of the console port. By default, the transmission rate is 9600 bit/s. The serial port supports the following transmission rates: • 9600bit/s • 19200bit/s • 38400bit/s • 57600bit/s • 115200bit/s After the transmission rate of the serial port is changed, change the transmission rate of the PC to be the same as that of the device and reconnect the PC and device.
0. Return	Return to the BootLoader menu.

14.5 Ethernet SubMenu

Access the BootLoader menu and select 3 to access the **Ethernet SubMenu**.

```
      BootLoader Menu

  1. Default Startup
  2. Serial SubMenu
  3. Ethernet SubMenu
  4. Modify Startup Parameters
  5. File System
  6. Password Manager
  7. Reboot

Enter your choice(1-7):3
                Ethernet SubMenu

  1. Update CPLD
  2. Update Software
  3. Display Parameters
  4. Modify Parameters
  5. Save Parameters
  0. Return

Enter your choice(0-5):
```

Table 14-3 Ethernet SubMenu

Item	Description
1. Update CPLD	Upgrade the CPLD through the network port.
2. Update Software	Upgrade the system software through the network port.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
3. Display Parameters	Modify network parameters through this menu.
4. Modify Parameters	Before uploading or downloading files, set network parameters through this menu. The configured network parameters take effect currently.
5. Save Parameters	To make the configured network parameters take effect during next restart, save the network parameters through this menu before device startup.
0. Return	Return to the BootLoader menu.

14.5.1 Modify Parameters

Access the Ethernet SubMenu and select **4** to access the **Modify Parameters** menu.

```
    Ethernet SubMenu

  1. Update CPLD
  2. Update Software
  3. Display Parameters
  4. Modify Parameters
  5. Save Parameters
  0. Return

Enter your choice(0-5):4
NOTE:
Ftp type define:  0(ftp), 1(tftp),
ENTER = no change; '.' = clear;

Ftp type           : 0
File name          : ar3600.cc
Ethernet ip address : 192.168.1.3
Ethernet ip mask    : 255.255.255.0
Host ip address     : 192.168.1.11
Ftp user           : huawei
Ftp password       : **********

Modify net parameter success.
```

- Run TFTP or FTP software on the PC. For details, see the third-party software help.

  NOTE

  You can use FTP or TFTP to set network parameters through this menu. The PC must function as the FTP or TFTP server and connects to the management port of the device, and the PC must be on the same network segment as the device.

- Set network parameters.

  The parameter values can contain only letters, numerals, underscores, and dots. Blanks are not allowed.

  – **Ftp type**: Configure the device as the FTP or TFTP client. By default, the device functions as the FTP client.

 Copyright © Huawei Technologies Co., Ltd.

- **File name**: Set the name of the file to be transferred.
- **Ethernet ip address**: Set the IP address of the management port.
- **Ethernet ip mask**: Set the subnet mask.
- **Host ip address**: Set the IP address of the FTP or TFTP server.
- **Ftp user**: Set the user name for accessing the FTP server.
- **Ftp password**: Set the password for accessing the FTP server.

NOTE

If the device uses TFTP to transfer files, press **Enter**. You do not need to set **Ftp user** and **Ftp password**.

14.6 Modify Startup Parameters

Access the BootLoader menu and select **4** to access the **Modify Startup Parameters** menu.

```
      BootLoader Menu

  1. Default Startup
  2. Serial SubMenu
  3. Ethernet SubMenu
  4. Modify Startup Parameters
  5. File System
  6. Password Manager
  7. Reboot

Enter your choice(1-7):4
            Modify Startup Parameters

  1. Display Current Startup Configuration
  2. Modify Startup Boot File
  3. Modify Startup Configuration File
  4. Startupfile Check Manage
  0. Return

Enter your choice(0-3):
```

Table 14-4 Modify Startup Parameters

Item	Description
1. Display Current Startup Configuration	View the system software and configuration file for current and next startup. Before system upgrade or downgrade, access this menu to check whether the system software and configuration file are correct.
2. Modify Startup Boot File	Specify system software for next startup. Before system upgrade or downgrade, access this menu to specify system software for next startup.
3. Modify Startup Configuration File	Specify the configuration file for next startup. Before system upgrade or downgrade, access this menu to specify the configuration file for next startup.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
4. Startupfile Check Manage	Manage the startup file check. To check or modify the startup file check configuration, access this menu to manage the startup file check.
0. Return	Return to the BootLoader menu.

14.6.1 Display Current Startup Configuration

Access the BootLoader menu and select **1** to access the **Display Current Startup Configuration** menu.

```
              Modify Startup Parameters

  1. Display Current Startup Configuration
  2. Modify Startup Boot File
  3. Modify Startup Configuration File
  4. Startupfile Check Manage
  0. Return

Enter your choice(0-3):1

************** Current Stratup info ****************
Valid Flag State       : Vaild
Boot File Name          : flash:/softwarenew.cc
Paf File Name          :
Licence File Name       :
Config File Name        : flash:/cfgnew.zip
Patch File Name         :

************** Pre Startup info ********************
Valid Flag State       : Vaild
Boot File Name          : flash:/software.cc
Paf File Name          :
Licence File Name       :
Config File Name        : flash:/cfg.zip
Patch File Name         :
```

You can access this menu to view the system software and configuration file for current and next startup.

14.6.2 Modify Startup Boot File

Access the BootLoader menu and select **2** to access the **Modify Startup Boot File** menu.

```
              Modify Startup Parameters

  1. Display Current Startup Configuration
  2. Modify Startup Boot File
  3. Modify Startup Configuration File
  4. Startupfile Check Manage
  0. Return

Enter your choice(0-3):2
        Select Boot File

  1. Flash
```

 Copyright © Huawei Technologies Co., Ltd.

```
  2. USB[0]
  0. Return

Enter your choice(0-2):1
NOTE: Boot file must be .cc or .CC

Current boot file: flash:/softwarenew.cc
Press ENTER directly for no change.
Or, please input the new file name: flash:/softwarenew1.cc
Save the boot file name: flash:/softwarenew1.cc ? Yes or No(Y/N)y
Save load state word...OK!
```

Before system upgrade or downgrade, access this menu to specify system software for next startup.

Select the flash memory or USB flash drive where the system software is stored. You can select the serial number.

If the check flag for the digital signature file of the system software is set based on **14.6.4 Startupfile Check Manage**, the procedure for specifying the startup system software is as follows:

```
            Modify Startup Parameters

  1. Display Current Startup Configuration
  2. Modify Startup Boot File
  3. Modify Startup Configuration File
  4. Startupfile Check Manage
  0. Return

Enter your choice(0-3):2
       Select Boot File

  1. Flash
  2. USB[0]
  0. Return

Enter your choice(0-2):1
NOTE: Boot file must be .cc or .CC

Current boot file: flash:/softwarenew.cc
Press ENTER directly for no change.
Or, please input the new file name: flash:/ar3600.cc
Save the boot file name: flash:/ar3600.cc ? Yes or No(Y/N)y
Signature Check needed!
       Select Signature file:
  0. Flash
  1. USB[1]

Enter your choice(0-1):0
Input the signature file: flash:/ar3600.cc.asc
 Verifying,This may last a few minutes.Please Wait.....
 Step1: Pre-deal with keyfile in start packet ...OK
 Step2: Pre-deal with applied signature file ...OK
 Step3: Pre-deal with target boot file ...OK
 Step4: Verifying Data.....OK
 signature file check success!

Signature check success!
Save the boot file name: falsh:/ar3600.cc ? Yes or No(Y/N) Y
Save load state word...OK!
```

14.6.3 Modify Startup Configuration File

Access the BootLoader menu and select **3** to access the **Modify Startup Configuration File** menu.

 Copyright © Huawei Technologies Co., Ltd.

```
            Modify Startup Parameters

  1. Display Current Startup Configuration
  2. Modify Startup Boot File
  3. Modify Startup Configuration File
  4. Startupfile Check Manage
  0. Return

Enter your choice(0-3):3
      Select Config File

  1. Flash
  2. USB[0]
  0. Return

Enter your choice(0-2):1
NOTE: Config file must be .zip or .cfg or .ZIP or .CFG

Current Config file: flash:/cfgnew.zip
Press ENTER directly for no change.
Or, please input the new file name: flash:/cfgnew1.zip
Save the config file name: flash:/cfgnew1.zip ? Yes or No(Y/N)y
Save load state word...OK!
```

When a specified configuration file is required to meet service requirements, you can use this menu to specify this configuration file for next startup.

Select the flash memory or USB flash drive where the configuration file is stored. You can select the serial number.

14.6.4 Startupfile Check Manage

Access the startup select submenu and select **4** to access the startup file check manage menu.

```
            Modify Startup Parameters

  1. Display Current Startup Configuration
  2. Modify Startup Boot File
  3. Modify Startup Configuration File
  4. Startupfile Check Manage
  0. Return

Enter your choice(0-3):4
      File Check Manage

  1. Set SignatureCheck Flag
  2. Clear SignatureCheck Flag
  3. Query SignatureCheck Flag
  0. return

Enter your choice(0-3):1
Set SignatureCheckFlag Success!

      File Check Manage

  1. Set SignatureCheck Flag
  2. Clear SignatureCheck Flag
  3. Query SignatureCheck Flag
  0. return

Enter your choice(0-3):3
StartUp SignatureCheck Flag Exist

      File Check Manage

  1. Set SignatureCheck Flag
```

 Copyright © Huawei Technologies Co., Ltd.

```
  2. Clear SignatureCheck Flag
  3. Query SignatureCheck Flag
  0. return

Enter your choice(0-3):2
Clear SignatureCheckFlag Success!

      File Check Manage

  1. Set SignatureCheck Flag
  2. Clear SignatureCheck Flag
  3. Query SignatureCheck Flag
  0. return

Enter your choice(0-3):3
StartUp SignatureCheck not Exist
```

To check or modify the system software check configuration, access this menu to manage the system software check.

Select **1. Set SignatureCheck Flag** to set the check flag for the digital signature file of the system software. The check flag is used for performing the validity check for the digital signature file of the system software. Select **2. Clear SignatureCheck Flag** to cancel the check flag for the digital signature file of the system software. Select **3. Query SignatureCheck Flag** to check whether the check flag for the digital signature file of the system software is set.

14.7 File System

Access the BootLoader menu and select **5** to access the **File System** menu.

```
      BootLoader Menu

  1. Default Startup
  2. Serial SubMenu
  3. Ethernet SubMenu
  4. Modify Startup Parameters
  5. File System
  6. Password Manager
  7. Reboot

Enter your choice(1-7):5
      File System

  1. Flash file system
  2. USB file system
  0. Return

Enter your choice(0-2):
```

Select **1** to access the **Flash file system** submenu. The flash file system is used as an example, and the USB flash drive file system is similar.

```
      File System

  1. Flash file system
  2. USB file system
  0. Return

Enter your choice(0-2):1
      Flash file system MENU

  1. List file in flash
  2. Delete file in flash
  3. Rename file in flash
```

 Copyright © Huawei Technologies Co., Ltd.

```
  4. Copy file in flash
  5. Format Flash file system
  6. Upload file to server
  7. Download file from server
  0. Return

Enter your choice(0-7):
```

- Select **1** to access the **List file in flash** submenu.

  ```
  Enter your choice(0-7):1
  Files in Directory of flash :
  total
  -rw-r--r--       242603520    Feb 20  11:11
  ar3600.cc
  -rw-r--r--       202317952    Feb 17  09:23
  ar3600_llt.cc
  drwx------            4096    Feb 19  15:16 logfile
  drwx------           16384    Feb 13  12:41 lost
  +found
  --w-------          304700    Feb 17  09:16
  sacrule.dat

   Total: 14636 MB, Used:  1229 MB, Free: 13407 MB ( 97%)
  ```

- Select **2** to access the **Delete file in flash** submenu.

  ```
  Enter your choice(0-7):2
  This may cause your system fail to start!
  Please input the file name you want to delete: sacrule.dat
  delete it? Yes or No(Y/N): y
  Deleting file[flash:/sacrule.dat], please wait....Done
  ```

- Select **3** to access the **Rename file in flash** submenu.

  ```
  Enter your choice(0-7):3
  Please input the file name: ar3600_llt.cc
  Please input the new name: ar3600_llt2.cc
  Rename file[flash:/ ar3600_llt.cc] to [flash:/ ar3600_llt2.cc], Yes or No(Y/N): y
  Rename OK!
  ```

- Select **4** to access the **Copy file in flash** submenu.

  ```
  Enter your choice(0-7):4
  Please input the file name:
  ar3600_llt2.cc
  Please input the new name:
  ar3600_llt3.cc
  Copy file[flash:/ar3600_llt2.cc] to [flash:/ar3600_llt3.cc], Yes or No(Y/N): y
  file copy OK!
  ```

- Select **5** to access the **Format Flash file system** submenu.

  ```
  Enter your choice(0-7):5
  All files in the device flash will be lost.
  Are you sure to format it? Yes or No(Y/N): y
  Format file system. Please wait....

  Format success!
  ```

- Select **6** to access the **Upload file to server** submenu.

  ```
  Enter your choice(0-7):6
  Please input the file name you want to upload:
  vrpcfg.zip
  upload file : vrpcfg.zip

  Reading file:[flash:/vrpcfg.zip], please
  wait ....done!

  Uploading[flash:/vrpcfg.zip] to server, please wait ....done
  ```

- Select **7** to access the **Download file from server** submenu.

  ```
  Enter your choice(0-7):7
  Please input the file name you want to download:
  ```

 Copyright © Huawei Technologies Co., Ltd.

```
grub.efi
download file : grub.efi

Downloading ....
file downloading is completed,writing file:[ flash:/grub.efi ]to file system .OK!
```

Table 14-5 File Manager menu

Item	Description
1. List file in flash/USB[0/1]	View the file list in the flash memory or USB flash drive.
2. Delete file in flash/USB[0/1]	Delete files from the flash memory or USB flash drive.
3. Rename file in flash/USB[0/1]	Rename directories or files in the flash memory or USB flash drive.
4. Copy file in flash/USB[0/1]	Copy directories or files in the flash memory or USB flash drive.
5. Format flash/USB[0/1] file system	Format the flash memory or USB flash drive.
6. Upload file to server	Upload files from the flash memory or USB flash drive to the server.
7. Download file from server	Download files from the server to the flash memory or USB flash drive.
0. Return	Return to the BootLoader menu.

14.8 Password Manager

Access the BootLoader menu and select **6** to access the **Password Manager** menu.

```
      BootLoader Menu

  1. Default Startup
  2. Serial SubMenu
  3. Ethernet SubMenu
  4. Modify Startup Parameters
  5. File System
  6. Password Manager
  7. Reboot

Enter your choice(1-7):6
      Password Manager

  1. Modify bootloader Password
  2. Clear the console login password
  0. Return

Enter your choice(0-2):1
Modify password. the password length must >= 6.Press Ctrl+c to
break.
Enter Old Password:******
Input new password:******
Input new password again:******
```

 Copyright © Huawei Technologies Co., Ltd.

```
Are you sure to change password? [y/n]:y
Save new password Success.

      Password Manager

  1. Modify bootloader Password
  2. Clear the console login password
  0. Return

Enter your choice(0-2):2
Clear the console login password Succeed!
```

To prevent unauthorized users from accessing the BootLoader menu, access the **Modify bootloader Password** menu to modify the password for accessing the BootLoader menu.

When you fail to log in to the device because the console port password is forgotten, access the **Clear the console login password** menu to delete the console port password.

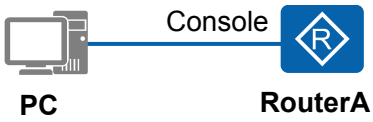
14.9 Configuration Examples for the BootLoader Menu on the AR3600

14.9.1 How to Log In to the Device Through the BootLoader If I Forget the Console Port Password

Networking Requirements

The console port of RouterA connects to the PC. When the console port password is forgotten, you can log in to the device through the BootLoader.

Figure 14-1 Logging in to the router through the BootLoader



Procedure

Step 1 Log in to the router through the console port.

NOTE

When performing operations, ensure that users on the serial port are kept online.

Step 2 Restart RouterA. Press **Ctrl+B** to access the BootLoader menu when the following information is displayed:

```
Bios    Version : V100R001C00B013
Created date of Bios : Nov 12 2014 - 14:06:29
```

 Copyright © Huawei Technologies Co., Ltd.

```
Memory Information:
      Memory Size : 24GB
      Memory Freq : DDR3-1333

Board Information:
      Intel(R) Xeon(R) CPU E5-1428L v2 @ 2.20GHz
      NumCores :  6
      Cpu Freq : 2214 MHz
      MicroCodeVers : 416
      CacheSize : 32
Pci Initializing...             ok
Usb Initializing...             ok
?
Boot from Main Grub

Grub    Version     : V100R001C00B013
Created date of Grub: Nov 19 2014 - 10:12:55

Press CTRL+S to enter grub shell ... 1



Boot from Main OS


Booting Linux Kernel.....
INIT: version 2.88 booting
Starting udev
Starting Bootlog daemon: bootlogd.
Populating dev cache

CPLD Version  : 100
Bios Version  : V100R001C00B013
Grub Version  : V100R001C00B013
Bootloader Version  : V100R001C00B013 Dec 12 2014
19:44:50

bootloader start!...
Press Ctrl+B to break auto startup ... 3
```

NOTE

Enter the password to access the BootLoader menu. The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

Step 3 Select **6** to access the **Password Manager** menu.

```
            BootLoader Menu

  1. Default Startup
  2. Serial SubMenu
  3. Ethernet SubMenu
  4. Modify Startup Parameters
  5. File System
  6. Password Manager
  7. Reboot

Enter your choice(1-7):6
```

Step 4 Select **2** to access the **Clear the console login password** menu.

```
      Password Manager

  1. Modify bootloader Password
  2. Clear the console login password
  0. Return

Enter your choice(0-2):2
```

 Copyright © Huawei Technologies Co., Ltd.

```
Clear the console login password Succeed!

    Password Manager

  1. Modify bootloader Password
  2. Clear the console login password
  0. Return

Enter your choice(0-2):0
```

Step 5 Select **1** to start the device. You will log in to the device after the start.

```
    BootLoader Menu

  1. Default Startup
  2. Serial SubMenu
  3. Ethernet SubMenu
  4. Modify Startup Parameters
  5. File System
  6. Password Manager
  7. Reboot

Enter your choice(1-7):1
```

----End

15 Android OS Management

About This Chapter

This document describes how to use and upgrade the Android OS and how to deploy applications in the Android OS.

NOTE

Only the AR161FW-P-M5 supports the Android OS.

15.1 Licensing Requirements and Limitations for Android OS Management
This section provides the configuration precautions of Android OS management function.

15.2 Logging In to and Operating the Android OS

15.3 Deploying APPs

15.4 System Upgrade

15.5 USB-based Deployment in the Android OS

15.6 FAQ About Android OS Management

15.1 Licensing Requirements and Limitations for Android OS Management

This section provides the configuration precautions of Android OS management function.

Involved Network Elements

None

Licensing Requirements

Android OS management function is a basic feature of a router and is not under license control.

 Copyright © Huawei Technologies Co., Ltd.

Feature Limitations

Only the AR161FW-P-M5 supports the Android OS.

15.2 Logging In to and Operating the Android OS

Prerequisites

The mouse, keyboard, and display have been prepared.

Procedure

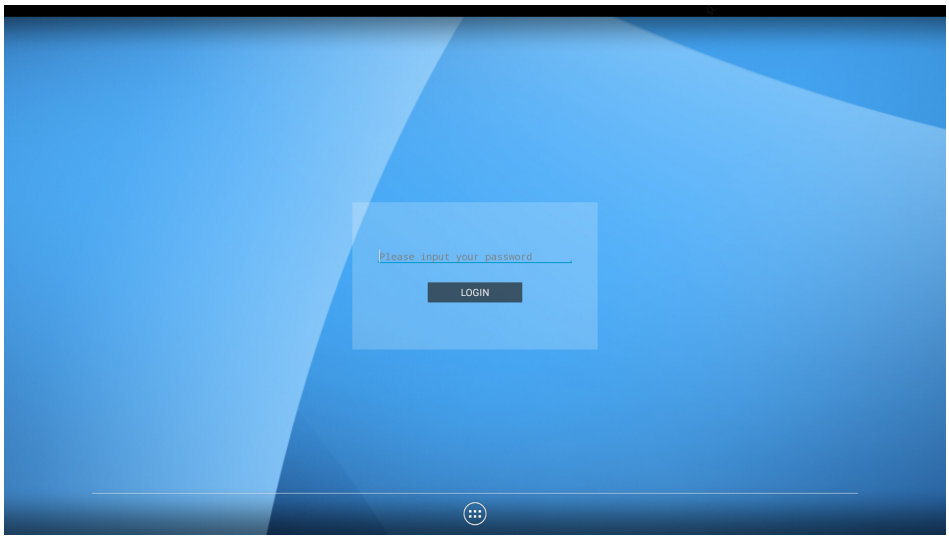
Step 1 Connect a mouse and a keyboard to the USB (Host) ports of the router.

NOTE

The AR161FW-P-M5 supports Bluetooth connections. You can connect the mouse and keyboard using Bluetooth.

Step 2 Connect the router to the display screen through a video cable. The router login page is displayed on the screen, as shown in **Figure 15-1**.

Figure 15-1 Router login page



Step 3 Enter the initial password. You successfully log in to the router, as shown in **Figure 15-2**. The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

 Copyright © Huawei Technologies Co., Ltd.

Figure 15-2 Router main page



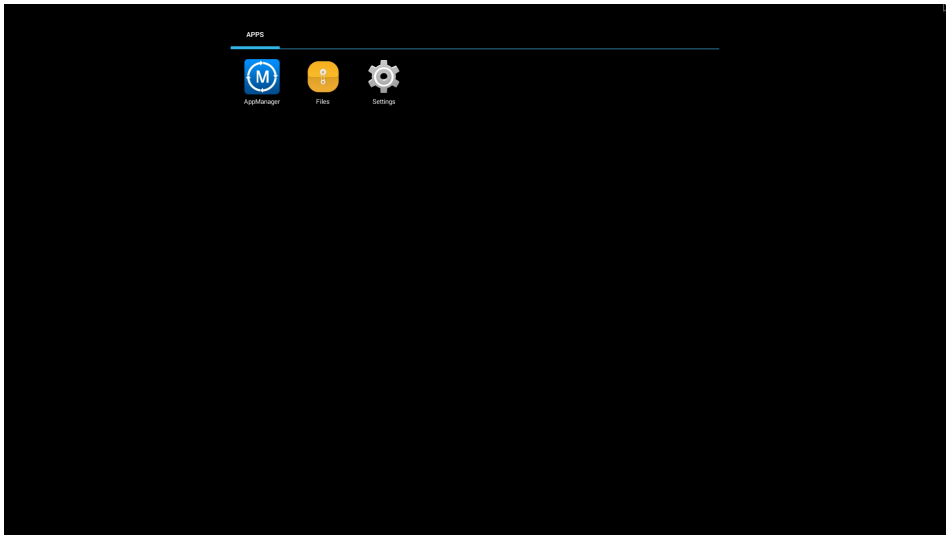
Step 4 Click  to access the **APPS** page, as shown in **Figure 15-3**.

NOTE

Use the keyboard and mouse to view and set menus on the **APPS** page of the router.

- You can right-click on the main interface to return to the upper-level menu.
- You can also press **ESC** to return to the upper-level menu.

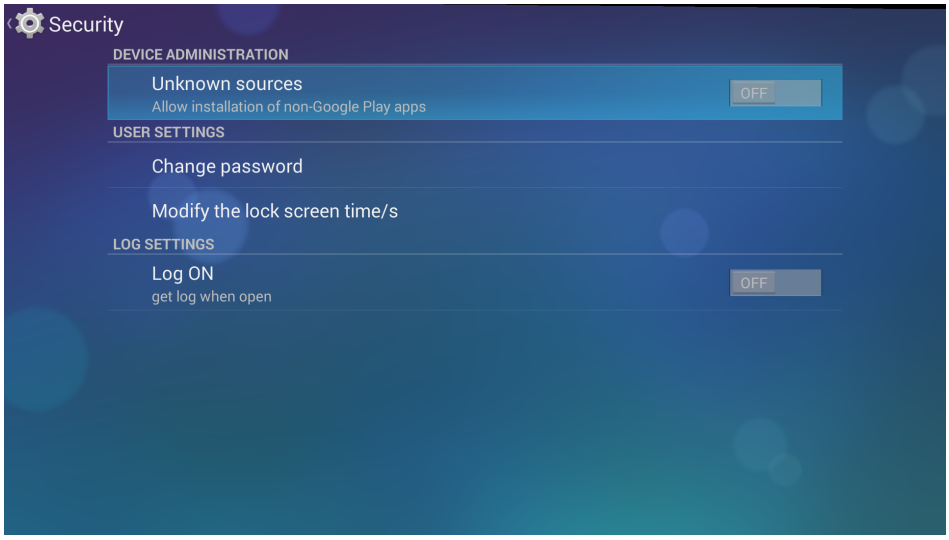
Figure 15-3 APPS page



Step 5 Configure the security settings of the router, as shown in **Figure 15-4**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 15-4 Security page



- Choose **Settings** > **Security** > **Change password** to change the login password.

  NOTE

  - The password must be a string of 8 to 22 characters.
  - A simple local user password may bring security risks, the user password must consist of two types of characters, including uppercase letters, lowercase letters, numerals, and special characters.

- Choose **Settings** > **Security** > **Modify the lock screen time/s** to set the screen lock timeout.

  NOTE

  By default, the screen lock timeout is 15 seconds.

- Choose **Settings** > **Security**. The security configuration page is displayed. In **Unknown sources**, set whether to allow installation of unknown applications to control the path where the applications are obtained.

----End

15.3 Deploying APPs

The APP deployment involves downloading, installing, updating, and uninstalling third-party APPs. To download, install, and update third-party APPs, you must remotely access the APP server for automatic operations. To uninstall third-party APPs, you can use the remote APP server for automatic uninstallation or manually perform the uninstallation operation on the Android OS.

APP Type

Table 15-1 describes the types of APPs on a router.

 Copyright © Huawei Technologies Co., Ltd.

Table 15-1 APP type

APP Type	Source	Supported Operations
System APP	Installed on a router before the router is delivered.	Update and uninstallation are not supported.
Third-party APP	Downloaded from third-party channels such as the APP server and website.	Download, installation, update, and uninstallation are supported.

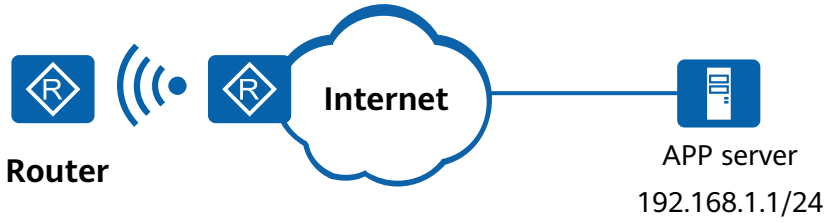
Preparation

Deploy an APP server

Deploy an APP server before remotely downloading, installing, updating, or uninstalling third-party APPs.

As shown in **Figure 15-5**, a router functions as a STA to access a remote APP server through a WLAN network.

Figure 15-5 Networking diagram for installing and deploying an APP server



Edit the APP detection file

Edit the APP detection file on the APP server and set APP information. The format of the APP detection file is as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<list>
<apk>
<name>com.busap.busapbackground</name>
<version>1.0</version>
<target>ARMaster</target>
<status>install</status>
<url>http://192.168.1.1/appmanager/apk/BusapBackground.apk</url>
<startinfo>com.busap.busapbackground,com.busap.busapbackground.MainActivity</startinfo>
</apk>
</list>
```

Table 15-2 Description of fields in the APP detection file

Field	Description
<list></list>	Indicates that the APP detection file is in the list format.

 Copyright © Huawei Technologies Co., Ltd.

Field	Description
<apk></apk>	Indicates that APP information is to be configured. **NOTE** To perform operations on multiple APPs, add this field in the APP detection file.
<name></name>	Specifies the APP software package name.
<version></version>	Specifies the APP version number. **NOTE** This field must be set to the same as the version of the APP to be installed, uninstalled, or updated. Otherwise, the router repeatedly installs, uninstalls, or upgrades this APP.
<target></target>	Specifies the model of the Android OS to which the APP belongs.
<status></status>	Specifies the type of the operation on the APP. The value can be: • **install**: When the status is install, the router checks whether the APP to be installed has been installed. If not, the router installs the APP. If so, the router compares whether the version of the installed APP is the same as that of the APP to be installed. If the versions are different, the router installs the APP. If the versions are the same, the router stops the installation. • **uninstall**: The router uninstalls the APP and does not detect the version number.
<url></url>	Specifies the URL from which the APP is downloaded.
<startinfo></startinfo>	Specifies information about automatic APP startup when the router starts. The format is <startinfo>*package name*, *path name and type name of the main activity to start*</startinfo>. To enable the APP to automatically start when the router starts, configure this field.

Set the directory for storing the APP

Store the APP in the specified directory on the APP server, which must be consistent with the directory specified by the **<url></url>** field in the APP detection file. In this example, the APP is stored in the **/appmanager/apk** directory of the root directory on the APP server.

Precautions

- If the router powers off or the network is disconnected during the remote APP download, the download process is interrupted. After the router is powered on

 Copyright © Huawei Technologies Co., Ltd.

or the network connection is recovered, the router redownloads the APP and overwrites the downloaded content.

- Before deploying an APP, ensure that the router has a reachable route to the APP server.
- Before deploying the APP, log in to the Android OS of the router. For the login procedure, see **15.2 Logging In to and Operating the Android OS**.

Processes of Remotely Downloading, Installing, Upgrading, and Uninstalling Third-Party APPs

The processes of remotely downloading, installing, upgrading, and uninstalling a third-party APP are described as follows.

1. Configure the URL of the APP detection file.
   a. Log in to the Android OS, open **AppManager**, and enter the URL specified by the **<url></url>** field in the APP detection file on the top address bar.

      You need to enter the URL only once, which will always stay on AppManager. If the **Automatic Detection of Upgrade** is enabled after the router starts, the router automatically starts this APP, and reads the APP detection file periodically or immediately when accessing the WLAN network. Based on the APP list defined in the APP detection file, the router can download, install, upgrade, and uninstall APPs.

      By default, the **Automatic Detection of Upgrade** is enabled.

   b. (Optional) Click **ADD**. The router starts detecting APPs.

      NOTE

      Perform this step when you want to immediately download, install, upgrade, or uninstall third-party APPs.
2. Download, install, upgrade, and uninstall a third-party APP.
   - Download and installation

     The router reads the APP detection file. When detecting that an APP with the operation type of **install** does not exist, the router automatically downloads the APP from the APP server and installs the APP in the internal storage.
   - Upgrade and installation

     The router reads the APP detection file. When detecting that an APP with the operation type of **install** has a different version from the local APP version, the router automatically downloads the APP of the latest version from the APP server and installs the APP in the internal storage.
   - Uninstallation

     The router reads the APP detection file. When detecting that an APP with the operation type of **uninstall** exists, the router automatically uninstalls the APP from the internal storage.
3. After the preceding operations are complete, search for the installed APP by choosing **All Applications** > **Installed Applications**, and check whether the router operates the APP according to the configuration in the APP detection file.

 Copyright © Huawei Technologies Co., Ltd.

Manually Uninstalling Third-Party APPs

In addition to uninstalling third-party APPs using the APP detection file, you can manually uninstall a third-party APP.

1. Log in to the Android OS, open **AppManager**, and click the third-party APP to be uninstalled.
2. Click **Uninstall**. In the displayed dialog box, click **OK**.
3. Choose **All Applications** > **Installed Applications** to check whether the APP is successfully uninstalled.

15.4 System Upgrade

15.4.1 Upgrading the System Using a USB Flash Drive

Preparation

Hardware environment

The hardware environment required for the upgrade is as follows:

- USB port: The AR161, AR161W, AR161EW, AR161EW-M1 routers provide USB 2.0 ports.
- USB flash drive:
  - Ensure that the USB flash drive is compatible with the router. Huawei-certified USB flash drives are recommended. The following USB flash drives have passed Huawei certification:
    - Netac: U208 (4 GB), U208S (16 GB)
    - Kingston: DT108, DT101 (8 GB), DTSE9 (8 GB, 16 GB)
    - SanDisk: CZ50 (8 GB, 16 GB), CZ36 (8 GB, 16 GB), CZ43 (16 GB)
    - HP: V250W (8 GB, 16 GB)
    - TOSHIBA: UHYBS-016GH/008GH
    - PNY: HOOK Gold Edition (16 GB, 32 GB)
  - The USB flash drive must use the FAT32 format; otherwise, set the format to FAT32 before using the USB flash drive.
  - The available space of the USB flash drive must be larger than the total size of files to be loaded.

Files to be loaded

Files to be loaded include:

- **update.zip**: indicates the target upgrade file, with the file name extension .zip.
- **unlmt.cfg**: indicates the unlimited upgrade in the period when the USB flash drive is installed.

 Copyright © Huawei Technologies Co., Ltd.

- **once.cfg**: indicates the one-time upgrade. That is, the system is upgraded only for once in the period when the USB flash drive is installed. This file is recommended for the system upgrade.

NOTE

To download **update.zip**, visit **http://support.huawei.com/enterprise** and log in using a registered user account. If you have no user account, click **Register** to apply for an account first. Choose **Software** > **Product Software** > **Enterprise Networking** > **Router** > **Access Router**. Download the system software matching the router.

The files **once.cfg** and **unlmt.cfg** are empty and used for the one-time upgrade and unlimited upgrade respectively. They are mutually exclusive.

Copy files

Create the **dload** folder in the root directory of the USB flash drive, and copy the files **update.zip** and **once.cfg**, or **update.zip** and **unlmt.cfg** to the **dload** folder.

NOTE

- Do not power off the router when the router is copying files. Otherwise, the upgrade fails or the router cannot start.
- Do not remove the USB flash drive before the upgrade is complete. Otherwise, data in the USB flash drive may be damaged.

Process

Install the USB flash drive and start the upgrade.

- One-time upgrade: After the USB flash drive is installed, the router checks whether the sizes of the **update.zip** files in use and in the USB flash drive are the same. If not, the router performs the upgrade. When the upgrade succeeds, the router automatically restarts and runs the upgrade **update.zip** file. In this case, the **update.zip** files in use and in the flash drive have the same size. The router does not perform an upgrade if restarted.
- Unlimited upgrade: After the USB flash drive is installed, the router automatically restarts and performs the upgrade without comparing the sizes of the **update.zip** files in use and in the USB flash drive. When the upgrade succeeds, the upgrade success message is displayed on the screen connected to the router. The router does not restart or upgrade. After the USB flash drive is removed, the router restarts. The upgrade is complete.

Verifying the Configuration

In the upgraded Android OS, choose **Settings** > **All Settings** > **SYSTEM** > **About AR** > **Android version** and check the version.

15.4.2 Upgrading the System Through the Upgrade Server

Preparation

Deploy an upgrade server

Before a remote upgrade, deploy an upgrade server first.

As shown in **Figure 15-6**, a router functions as a STA to access a remote upgrade server through a WLAN network.

 Copyright © Huawei Technologies Co., Ltd.

Figure 15-6 Networking diagram for remotely connecting a router to an upgrade server



Files to be loaded

Files to be loaded for the upgrade include the upgrade file of the Android OS, with the file name extension .zip. The name of the upgrade file is **update.zip**.

NOTE

To download **update.zip**, visit **http://support.huawei.com/enterprise** and log in using a registered user account. If you have no user account, click **Register** to apply for an account first. Choose **Software** > **Product Software** > **Enterprise Networking** > **Router** > **Access Router**. Download the system software matching the router.

Edit the upgrade detection file

Edit the upgrade detection file on the upgrade server and set upgrade information. The format of the upgrade detection file is as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<list>
<update>
<target>AR</target>
<version>V200R005C30SPC100</version>
<urlemmc>http://www.example.com/appmanager/update/update.zip</urlemmc>
</update>
</list>
```

Table 15-3 Description of fields in the upgrade detection file

Field	Description
<list></list>	Indicates that the upgrade detection file is in the list format.
<update></update>	Indicates that upgrade information is to be configured. **NOTE** To remotely upgrade multiple routers, add this field in the upgrade detection file.
<target></target>	Specifies the name of the device to be upgraded. This field specifies the device to be upgraded.

 Copyright © Huawei Technologies Co., Ltd.

Field	Description
<version></version>	Specifies the target version. **NOTE** This field must be set to the same as the version in the upgrade file to be downloaded. Otherwise, the system is repeatedly upgraded.
<urlemmc></urlemmc>	Specifies the eMMC URL from which the upgrade file is downloaded.

Set the directory for storing the upgrade file

Store the upgrade file in the specified directory on the upgrade server, which must be consistent with the directory specified by the **<url></url>** field in the upgrade detection file. In this example, the upgrade file is stored in the **/appmanager/apk** directory of the root directory on the upgrade server.

Precautions

- If the router powers off or the network is disconnected during the upgrade file download, the download process is interrupted. After the router is powered on or the network connection is recovered, the router continues to download the upgrade file but does not redownload the upgrade file. If the upgrade file after the power-off changes, the new upgrade file overrides the downloaded one.
- Before performing an upgrade, ensure that the router has a reachable route to the upgrade server.
- Before performing an upgrade, log in to the Android OS of the router. For the login procedure, see **15.2 Logging In to and Operating the Android OS**.

Process

The upgrade process is as follows:

1. Configure the URL of the upgrade detection file.
   a. Log in to the Android OS, open **AppManager**, and enter the URL specified by the **<url></url>** field in the upgrade detection file on the top address bar.

      You need to enter the URL only once, which will always stay on the application manager. After startup, the router automatically performs the upgrade and reads the upgrade detection file periodically or immediately when accessing the WLAN network. If the current version is different from the target version, the upgrade flag is not set, and the router is not performing the download or upgrade operation, the router automatically downloads the upgrade file.
   b. (Optional) Click **ADD**. The router starts detecting the upgrade and download the upgrade file.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Perform this step when you want to immediately upgrade the Android OS and system software.

2. Upgrade the system.

   Store the upgrade file to the upgrade directory and set the upgrade flag. Upon the next startup, the router performs the upgrade when detecting the upgrade flag.

Verifying the Configuration

In the upgraded Android OS, choose **Settings** > **All Settings** > **SYSTEM** > **About AR** > **Android version** and check the version.

15.5 USB-based Deployment in the Android OS

Pre-configuration Tasks

The device provides a USB 2.0 interface. Before configuring USB-based deployment in the Android operating system (OS), prepare the following hardware environment:

- USB flash drive
  - Ensure that the USB flash drive is compatible with the device. Huawei-certified USB flash drives are recommended. Currently, the following USB flash drives have passed Huawei certification:
    - Netac: U208 (4 GB), U208S (16 GB)
    - Kingston: DT108, DT101 (8 GB), and DTSE9 (8 GB and 16 GB)
    - SanDisk: CZ50 (8 GB and 16 GB), CZ36 (8 GB and 16 GB), and CZ43 (16 GB)
    - HP: V250W (8 GB and 16 GB)
    - Toshiba: UHYBS-016GH/008GH
    - PNY: Golden Hook (16 GB and 32 GB)
  - The USB flash drive must use the FAT32 format; otherwise, set the format to FAT32 before using the USB flash drive.
  - The available space of the USB flash drive must be larger than the total size of files to be loaded.
- Mouse, keyboard, and display

  Perform USB-based deployment after the Android OS runs properly.

Context

The device supports USB-based deployment using the Android OS software and configuration file.

 Copyright © Huawei Technologies Co., Ltd.

- If only the Android OS software is used, the deployment files are **update.zip** and **once.cfg**, or **update.zip** and **unlmt.cfg**.
- If only the configuration file is used, the deployment files are **osp_settings.db** and **once.cfg**, **osp_settings.db** and **unlmt.cfg**, **osp_settings.zip** and **once.cfg**, or **osp_settings.zip** and **unlmt.cfg**.

  NOTE

  Only AR161FW-P-M5 and AR169-P-M9 supports this function.
- If both the Android OS software and configuration file are used, the deployment files are one of the following combinations:
  - **update.zip**, **osp_settings.db**, and **once.cfg**
  - **update.zip**, **osp_settings.db**, and **unlmt.cfg**
  - **update.zip**, **osp_settings.zip**, and **once.cfg**
  - **update.zip**, **osp_settings.zip**, and **unlmt.cfg**

  NOTE

  Only AR161FW-P-M5 and AR169-P-M9 supports this function.

NOTE

The files **once.cfg** and **unlmt.cfg** are empty text files used for one-time upgrade and unlimited upgrade respectively. The two files are mutually exclusive.

The file **osp_settings.db** can only be used for the first USB-based deployment when the device does not have a compression password for USB-based deployment (no compression password is configured when the device is delivered). If the file **osp_settings.zip** is used for USB-based deployment, the device must have the compression password for USB-based deployment. For details about how to set the password, see **15.5.4 Setting the Password of the Compressed Configuration File for USB-based Deployment**. The files **osp_settings.db** and **osp_settings.zip** are mutually exclusive.

Configuration Process

If only the Android OS software is used, see **15.5.1 USB-based Deployment Using Only the Android OS Software** for the deployment process. If only the configuration file is used, see **15.5.2 USB-based Deployment Using Only the Configuration File** for the deployment process. If both the Android OS software and configuration file are used, see **15.5.3 USB-based Deployment Using the Android OS Software and Configuration File** for the deployment process.

15.5.1 USB-based Deployment Using Only the Android OS Software

Preparation

Files to Be Loaded

The following files need to be loaded:

- **update.zip**: indicates the target Android OS upgrade file, with the file name extension .zip.
- **unlmt.cfg**: indicates the unlimited upgrade. If this file is loaded, the device with the USB flash drive installed can be upgraded repeatedly.

 Copyright © Huawei Technologies Co., Ltd.

- **once.cfg**: indicates the one-time upgrade. If this file is loaded, the device with the USB flash drive installed is upgraded only once. After the upgrade succeeds, the device will not be upgraded again.

NOTE

To download **update.zip**, visit **http://support.huawei.com/enterprise** and log in using a registered user account. If you do not have a user account, click **Register** to apply for an account first. Choose **Downloads** > **Enterprise Networking** > **Enterprise Gateway** > **Application Router**. Download the Android OS software based on the device model and version.

The files **once.cfg** and **unlmt.cfg** are two empty text files created by users. The two files are mutually exclusive.

Copying Files

Create the folder **dload** in the root directory of the USB flash drive, and copy the files **update.zip** and **once.cfg**, or **update.zip** and **unlmt.cfg** to the folder **dload**.

Upgrade Process

After the Android OS runs properly and you log in the system, install the USB flash drive and start the upgrade.

NOTE

- Do not power off the device when the device is copying files. Otherwise, the upgrade may fail or the device cannot start.
- Do not remove the USB flash drive before the upgrade is complete. Otherwise, data in the USB flash drive may be damaged.
- Do not install multiple USB flash drives simultaneously for USB-based deployment.

- One-time upgrade: After the USB flash drive is installed, the device checks whether the sizes (byte-level precision) of the file **update.zip** in use and that in the USB flash drive are the same. If not, the device performs the upgrade. After the upgrade succeeds, the device automatically restarts and runs the upgrade file **update.zip**. In this case, the file **update.zip** in use and that in the USB flash drive have the same size. The device will not perform an upgrade if it restarts.
- Unlimited upgrade: After the USB flash drive is installed, the device automatically restarts and performs the upgrade without comparing the sizes of the file **update.zip** in use and that in the USB flash drive. After the upgrade succeeds, an upgrade success message is displayed on the screen connected to the device. The device does not restart or keep upgrading. After the USB flash drive is removed, the device restarts, and the upgrade is complete.

Verifying the Configuration

In the Android OS, choose **Settings** > **ALL settings** > **SYSTEM** > **About AR** > **Android version** and check whether the Android version changes after the upgrade.

 Copyright © Huawei Technologies Co., Ltd.

15.5.2 USB-based Deployment Using Only the Configuration File

Preparation

Files to Be Loaded

The following files need to be loaded:

- **osp_settings.db**: indicates the target Android OS configuration file, with the file name extension .db.
- **osp_settings.zip**: indicates the target Android OS configuration file, with the file name extension .zip.
- **unlmt.cfg**: indicates the unlimited upgrade. If this file is loaded, the device with the USB flash drive installed can be upgraded repeatedly.
- **once.cfg**: indicates the one-time upgrade. If this file is loaded, the device with the USB flash drive installed is upgraded only once. After the upgrade succeeds, the device will not be upgraded again.

NOTE

The file **osp_settings.db** can only be used for the first USB-based deployment when the device does not have a compression password for USB-based deployment (no compression password is configured when the device is delivered). The file **osp_settings.zip** is an encrypted and compressed configuration file. If the file **osp_settings.zip** is used for USB-based deployment, the device must have the compression password for USB-based deployment. The files **osp_settings.db** and **osp_settings.zip** are mutually exclusive.

Currently, the device supports only the following two encryption modes:

- Simple text encryption: For example, when you compress a .db configuration file into a .zip file, you can enter a password in the compression software to encrypt the configuration file.
- AES256 encryption algorithm: For example, when you compress a .db configuration file into a .zip file, you can select the AES256 mode and enter a password in the compression software to encrypt the configuration file. This encryption mode is recommended because it is more secure.

To improve security, you are advised to encrypt the configuration file to be loaded. The encryption password of the configuration file must be the same as the password of the compressed configuration file for USB-based deployment on the device. For details about how to configure the password of the compressed configuration file, see **15.5.4 Setting the Password of the Compressed Configuration File for USB-based Deployment**.

The files **once.cfg** and **unlmt.cfg** are two empty text files created by users. The two files are mutually exclusive.

Copying Files

Create the folder **dload** in the root directory of the USB flash drive, and copy the files **osp_settings.db** and **once.cfg**, **osp_settings.db** and **unlmt.cfg**, **osp_settings.zip** and **once.cfg**, or **osp_settings.zip** and **unlmt.cfg** to the folder.

USB-based Deployment Process

After the device runs properly, install the USB flash drive and start the upgrade.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- Do not power off the device when the device is copying files. Otherwise, the USB-based deployment may fail or the device cannot start.
- Do not remove the USB flash drive before the device restarts. Otherwise, data in the USB flash drive may be damaged or the USB-based deployment may fail.
- Do not install multiple USB flash drives simultaneously for USB-based deployment.

- Configuration file: **osp_settings.db**

  This file can only be used for the first USB-based deployment when the device does not have the password of the compressed configuration file for USB-based deployment. The deployment files can be **osp_settings.db** and **once.cfg**, or **osp_settings.db** and **unlmt.cfg**.

  The file **osp_settings.db** needs to carry the password of the compressed configuration file for the second USB-based deployment. The password is used for decompressing the configuration file **osp_settings.zip** in future USB-based deployments.

  After the USB flash drive is installed, the device copies the configuration file **osp_settings.db**. After the USB-based deployment is complete, the device automatically restarts. After the device restarts and displays the Android OS login page, remove the USB flash drive.
- Configuration file: **osp_settings.zip**

  This file applies to USB-based deployment scenarios where the device has the password of the compressed configuration file.

  – One-time USB-based deployment using the deployment files **osp_settings.zip** and **once.cfg**

    After the USB flash drive is installed, the device checks whether the timestamp on the device is the same as that in the configuration file **osp_settings.zip**. If not, the device decompresses and loads the configuration file **osp_settings.zip**. After the device restarts and displays the Android OS login page, remove the USB flash drive.

  – Unlimited USB-based deployment using the deployment files **osp_settings.zip** and **unlmt.cfg**

    After the USB flash drive is installed, the device decompresses the configuration file **osp_settings.zip** and automatically restarts. After the device restarts and displays the Android OS login page, remove the USB flash drive.

15.5.3 USB-based Deployment Using the Android OS Software and Configuration File

Preparation

Files to Be Loaded

The following files need to be loaded:

- **update.zip**: indicates the target Android OS upgrade file, with the file name extension .zip.
- **osp_settings.db**: indicates the target Android OS configuration file, with the file name extension .db.

 Copyright © Huawei Technologies Co., Ltd.

- **osp_settings.zip**: indicates the target Android OS configuration file, with the file name extension .zip.
- **unlmt.cfg**: indicates the unlimited upgrade. If this file is loaded, the device with the USB flash drive installed can be upgraded repeatedly.
- **once.cfg**: indicates the one-time upgrade. If this file is loaded, the device with the USB flash drive installed is upgraded only once. After the upgrade succeeds, the device will not be upgraded again.

NOTE

The file **osp_settings.db** can only be used for the first USB-based deployment when the device does not have a compression password for USB-based deployment (no compression password is configured when the device is delivered). The file **osp_settings.zip** is an encrypted and compressed configuration file. If the file **osp_settings.zip** is used for USB-based deployment, the device must have the compression password for USB-based deployment. The files **osp_settings.db** and **osp_settings.zip** are mutually exclusive.

Currently, the device supports only the following two encryption modes:

- Simple text encryption: For example, when you compress a .db configuration file into a .zip file, you can enter a password in the compression software to encrypt the configuration file.
- AES256 encryption algorithm: For example, when you compress a .db configuration file into a .zip file, you can select the AES256 mode and enter a password in the compression software to encrypt the configuration file. This encryption mode is recommended because it is more secure.

To improve security, you are advised to encrypt the configuration file to be loaded. The encryption password of the configuration file must be the same as the password of the compressed configuration file for USB-based deployment on the device. For details about how to configure the password of the compressed configuration file, see **15.5.4 Setting the Password of the Compressed Configuration File for USB-based Deployment**.

The files **once.cfg** and **unlmt.cfg** are two empty text files created by users. The two files are mutually exclusive.

Copying Files

Create the folder **dload** in the root directory of the USB flash drive, and copy one of the following deployment file combinations to the folder:

- **update.zip**, **osp_settings.db**, and **once.cfg**
- **update.zip**, **osp_settings.db**, and **unlmt.cfg**
- **update.zip**, **osp_settings.zip**, and **once.cfg**
- **update.zip**, **osp_settings.zip**, and **unlmt.cfg**

USB-based Deployment Process

After the Android OS runs properly and you log in the system, install the USB flash drive and start the USB-based deployment.

NOTE

- Do not power off the device when the device is copying files. Otherwise, the USB-based deployment may fail or the device cannot start.
- Do not remove the USB flash drive before the USB-based deployment is complete. Otherwise, data in the USB flash drive may be damaged or the USB-based deployment may fail.
- Do not install multiple USB flash drives simultaneously for USB-based deployment.

 Copyright © Huawei Technologies Co., Ltd.

- Deployment files: **update.zip**, **osp_settings.db**, and **once.cfg**

  These files can only be used for the first USB-based deployment when the device does not have the password of the compressed configuration file for USB-based deployment.

  After the USB flash drive is installed, the device checks whether the sizes (byte-level precision) of the file **update.zip** in use and that in the USB flash drive are the same. If not, the device performs the upgrade and copies the configuration file **osp_settings.db**. After the deployment succeeds, the device automatically restarts. After the device restarts and displays the Android OS login page, remove the USB flash drive.

- Deployment files: **update.zip**, **osp_settings.db**, and **unlmt.cfg**

  These files can only be used for the first USB-based deployment when the device does not have the password of the compressed configuration file for USB-based deployment.

  After the USB flash drive is installed, the device automatically performs the upgrade without comparing the sizes of the file **update.zip** in use and that in the USB flash drive, and copies the configuration file **osp_settings.db**. After the upgrade succeeds, an upgrade success message is displayed on the screen connected to the device. The device does not restart and will not be deployed repeatedly. After the USB flash drive is removed, the device restarts, and the deployment is complete.

- Deployment files: **update.zip**, **osp_settings.zip**, and **once.cfg**

  These files apply to scenarios where the device have the password of the compressed configuration file for USB-based deployment. For details about how to set the password, see **15.5.4 Setting the Password of the Compressed Configuration File for USB-based Deployment**.

  After the USB flash drive is installed, the device checks whether the sizes (byte-level precision) of the file **update.zip** in use and that in the USB flash drive are the same. If not, the device upgrades the Android OS software.

  The device checks whether the timestamp on the device is the same as that in the configuration file **osp_settings.zip**. If not, the device decompresses and loads the configuration file **osp_settings.zip** to the device.

  After the deployment succeeds, the device restarts and displays the Android OS login page, remove the USB flash drive.

- Deployment files: **update.zip**, **osp_settings.zip**, and **unlmt.cfg**

  These files apply to scenarios where the device have the password of the compressed configuration file for USB-based deployment. For details about how to set the password, see **15.5.4 Setting the Password of the Compressed Configuration File for USB-based Deployment**.

  After the USB flash drive is installed, the device automatically performs the upgrade without comparing the sizes of the file **update.zip** in use and that in the USB flash drive, and decompresses the configuration file **osp_settings.zip**. After the deployment succeeds, an upgrade success message is displayed on the screen connected to the device. The device does not restart and will not be deployed repeatedly. After the USB flash drive is removed, the device restarts, and the deployment is complete.

 Copyright © Huawei Technologies Co., Ltd.

Verifying the Configuration

In the Android OS, choose **Settings** > **ALL settings** > **SYSTEM** > **About AR** > **Android version** and check whether the Android version changes after the upgrade.

15.5.4 Setting the Password of the Compressed Configuration File for USB-based Deployment

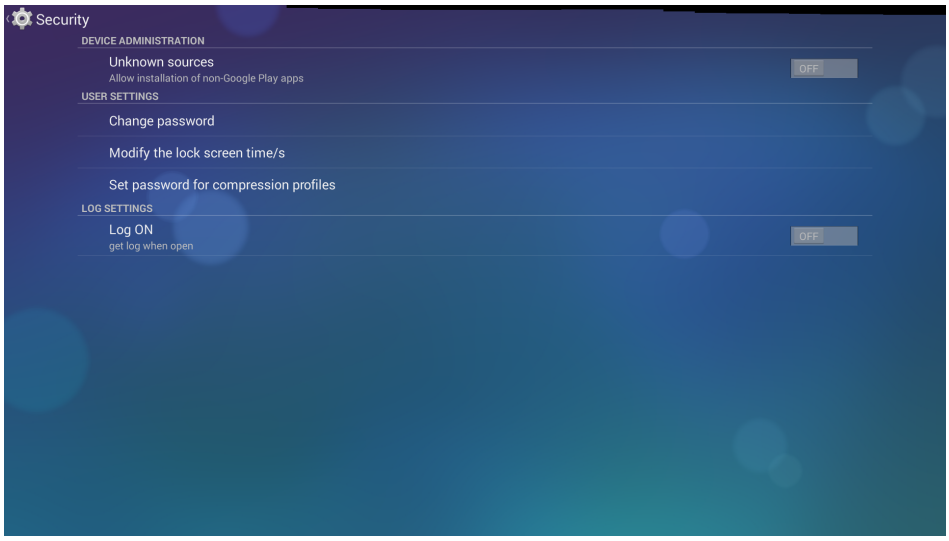
Context

If the configuration file **osp_settings.zip** is used for USB-based deployment, the password for the configuration file **osp_settings.zip** must be the same as the password of the compressed configuration file for USB-based deployment in the Android OS on the device; otherwise, the USB-based deployment fails. In the first USB-based deployment, if the device does not contain the password of the compressed configuration file for USB-based deployment in the Android OS or the password is forgotten, you need to perform the following operations to set the password.

Procedure

Step 1 Choose **Settings** > **Security**. The **Security** page is displayed, as shown in **Figure 15-7**.

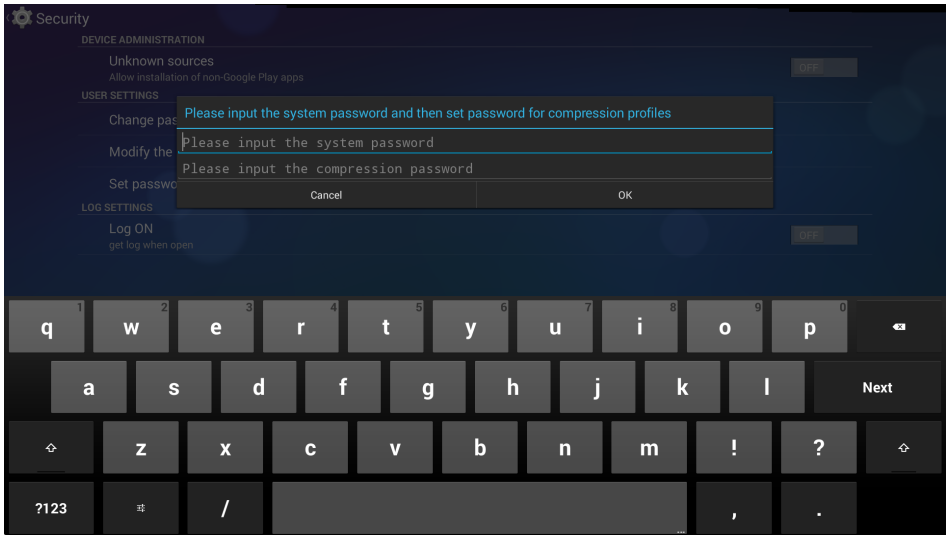
Figure 15-7 Security page



Step 2 Click **Set password for compression profiles**. In the dialog box that is displayed, enter the Android OS login password and the password of the compressed configuration file for USB-based deployment in the Android OS, and click **OK**, as shown in **Figure 15-8**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 15-8 Setting the password of the compressed configuration file for USB-based deployment



----End

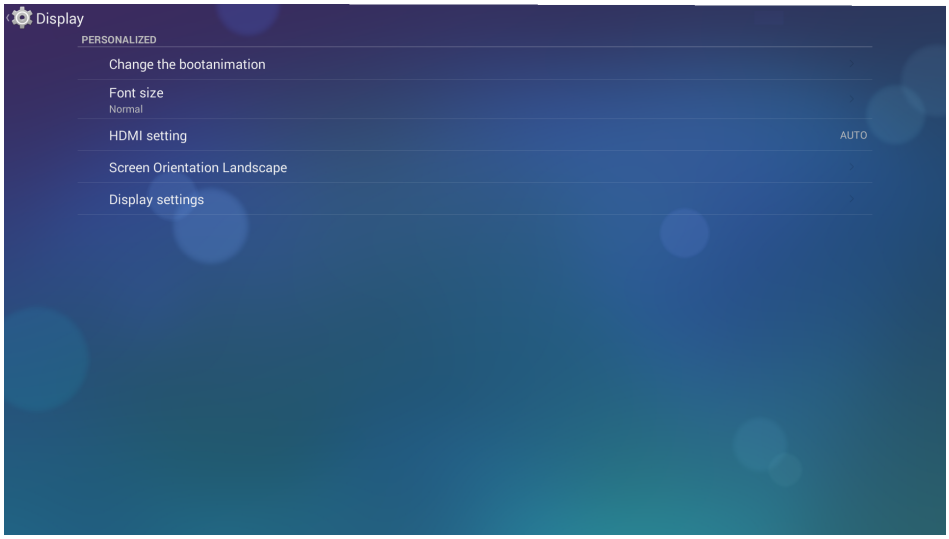
15.6 FAQ About Android OS Management

15.6.1 How Do I Configure the Screen Rotation Function?

Procedure

Step 1 Choose **Settings** > **Display**. The **PERSONALIZED** page is displayed, as shown in Figure 15-9.

Figure 15-9 Personalized page



Step 2 Click **Screen Orientation Landscape**. The **Landscape settings** dialog box is displayed. Click **OK** to configure the screen rotation function. The function takes effect after the device restarts.

----End

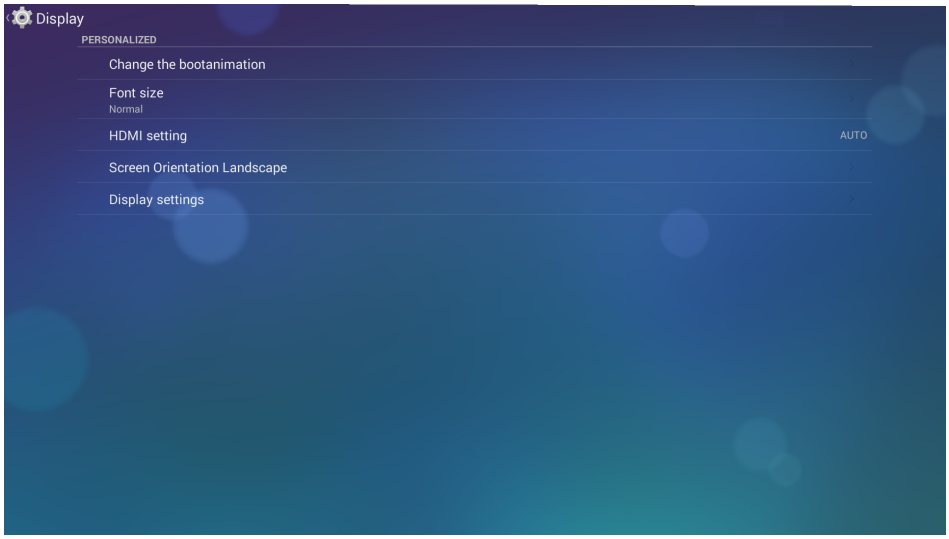
15.6.2 How Do I Set the Screen Resolution?

A proper resolution ensures good visual effect.

Procedure

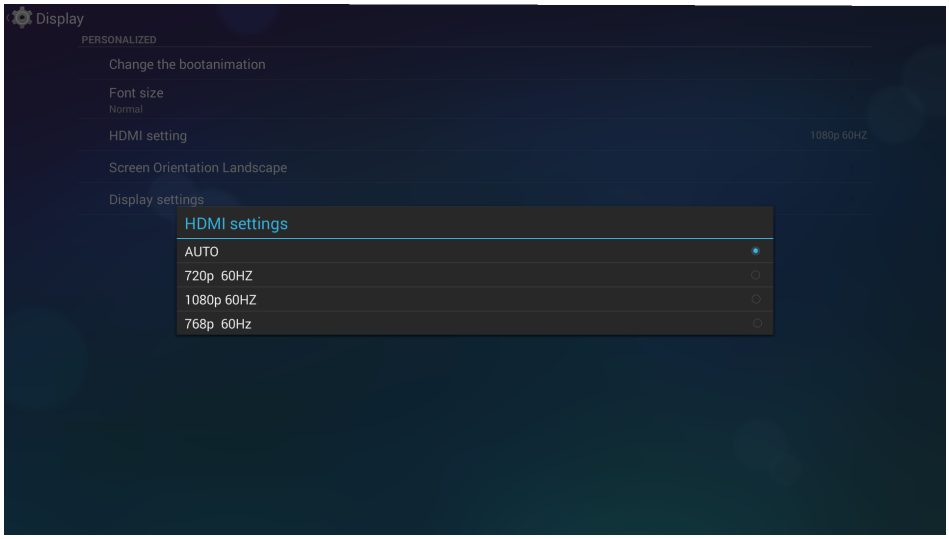
Step 1 Choose **Settings** > **Display**. The **PERSONALIZED** page is displayed, as shown in **Figure 15-10**.

Figure 15-10 Personalized page



Step 2 Click **HDMI setting**. Select the screen resolution in the **HDMI settings** dialog box that is displayed, as shown in **Figure 15-11**.

Figure 15-11 HDMI settings dialog box



 Copyright © Huawei Technologies Co., Ltd.

Step 3 After the screen resolution is selected, the system displays a dialog box. Click **ok**. The device restarts immediately. The configured screen resolution takes effect after the device restarts. If you click **cancel** or do not click **ok** within 10 seconds, the system restores the original screen resolution.

----End

15.6.3 How Do I Configure Display Settings?

Context

The **Display settings** dialog box provides three options: **Lock aspect ratio**, **Stretch to full screen**, and **Manual**.

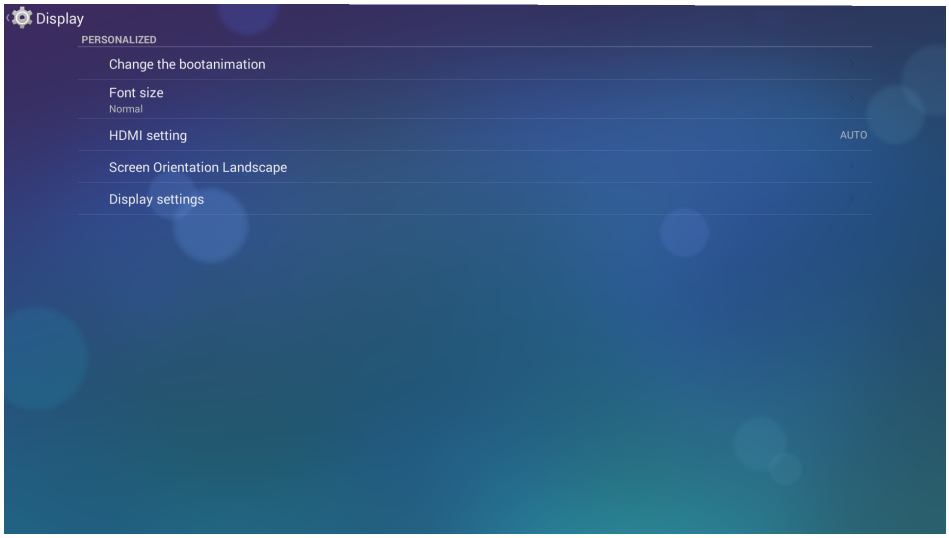
- **Lock aspect ratio**: A page is displayed in the normal aspect ratio. Most televisions use this mode.
- **Stretch to full screen**: This mode applies to displays. A page is displayed in full screen mode. If the page is not displayed in full screen mode or cannot be displayed clearly, select this mode to adjust the display effect.
- **Manual**: You can manually adjust the display effect based on the display or television.

Configure display settings based on the actual situation.

Procedure

Step 1 Choose **Settings** > **Display**. The **PERSONALIZED** page is displayed, as shown in Figure 15-12.

Figure 15-12 Personalized page

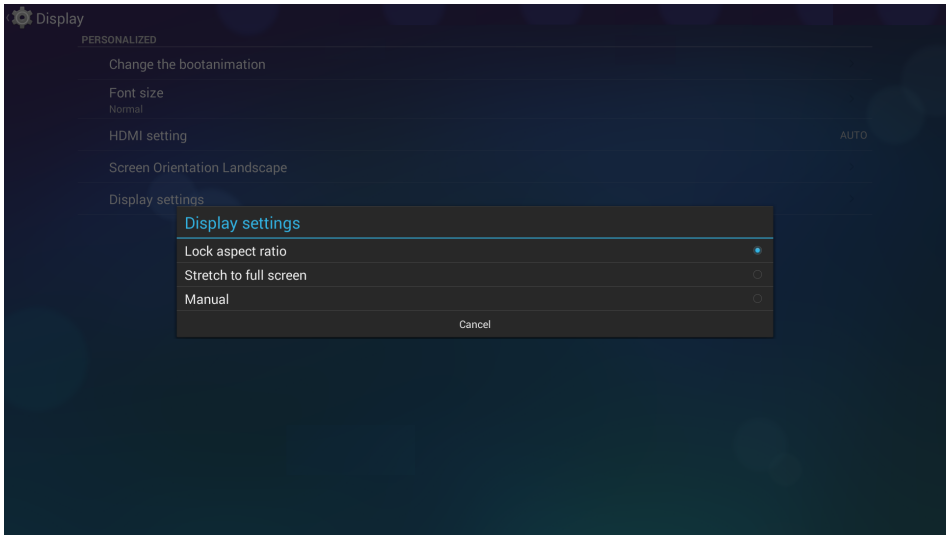


Step 2 Click **Display settings**. Set the display in the **Display settings** dialog box that is displayed.

- If you select **Lock aspect ratio** or **Stretch to full screen**, the configuration takes effect immediately.
- If you select **Manual**, go to **Step 3**.

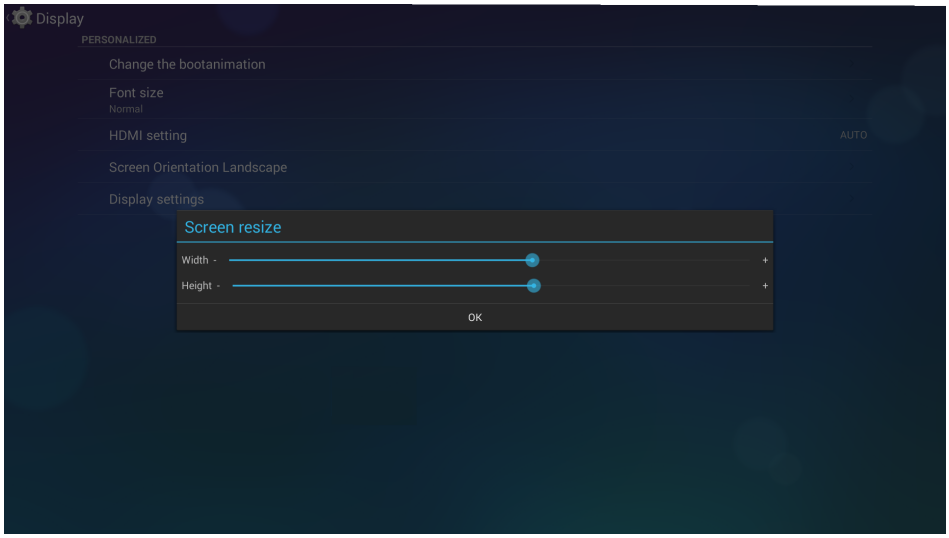
 Copyright © Huawei Technologies Co., Ltd.

Figure 15-13 Display settings dialog box



Step 3 Click **Manual**. The **Screen resize** dialog box is displayed. Set the width and height based on actual display requirements, and click **OK**, as shown in **Figure 15-14**. The configuration takes effect.

Figure 15-14 Screen resize dialog box



----End

What If the Page Is Not Displayed in Full Screen or Cannot Be Displayed Clearly?

The solution is as follows:

1. Select **Stretch to full screen** to adjust the display effect.
2. If the image is beyond the display range after you select **Stretch to full screen**, the problem is caused by the display device. In this case, you can adjust the display device. The adjustment methods vary according to different display devices. Make correct adjustments according to the specific model.

 Copyright © Huawei Technologies Co., Ltd.

16 Smart Upgrade Configuration

About This Chapter

16.1 Overview of Smart Upgrade

16.2 Smart Upgrade Process

16.3 Licensing Requirements and Limitations for Smart Upgrade

16.4 Configuring Smart Upgrade

16.5 Example for Configuring Smart Upgrade

16.1 Overview of Smart Upgrade

Definition

Smart upgrade refers to the process of automatically upgrading devices by connecting them to the Huawei Online Upgrade Platform (HOUP) through the Internet.

Purpose

As network scales enlarge, an increasing number of devices are deployed on the network, and users using traditional device upgrade modes suffer from the following pain points:

- Complicated and time-consuming upgrade procedure
- Laborious because of frequent software version upgrades
- Dispersed device locations, resulting in high communication costs for resource coordination

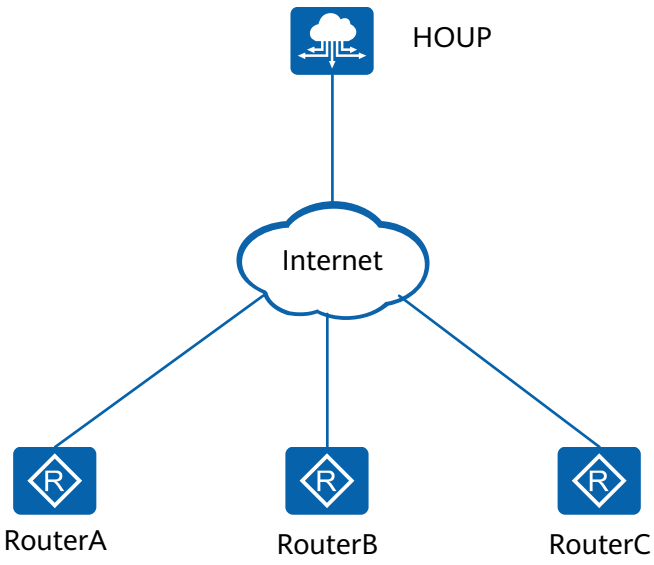
To free users from such pain points and enable them to upgrade devices more conveniently, smart upgrade is developed. Smart upgrade achieves online automatic upgrade of devices by connecting them to the HOUP, simplifying the upgrade procedure, improving maintenance efficiency, and reducing O&M costs.

 Copyright © Huawei Technologies Co., Ltd.

16.2 Smart Upgrade Process

To implement smart upgrade, connect devices to the HOUP through the Internet, as shown in **Figure 16-1**. A smart upgrade-enabled AR router periodically sends its own information, including the device model, ESN, current system software version, and current patch, to the HOUP. The HOUP returns the latest version information, including the recommended system software version, patch, patch type, and download path, to the router based on the maintenance policy. You can determine whether to upgrade the router immediately or at a scheduled time based on the returned information. The router then automatically downloads the software package and performs an upgrade accordingly. After the upgrade is completed, the router reports the upgrade result to the HOUP.

Figure 16-1 Networking diagram for deploying smart upgrade

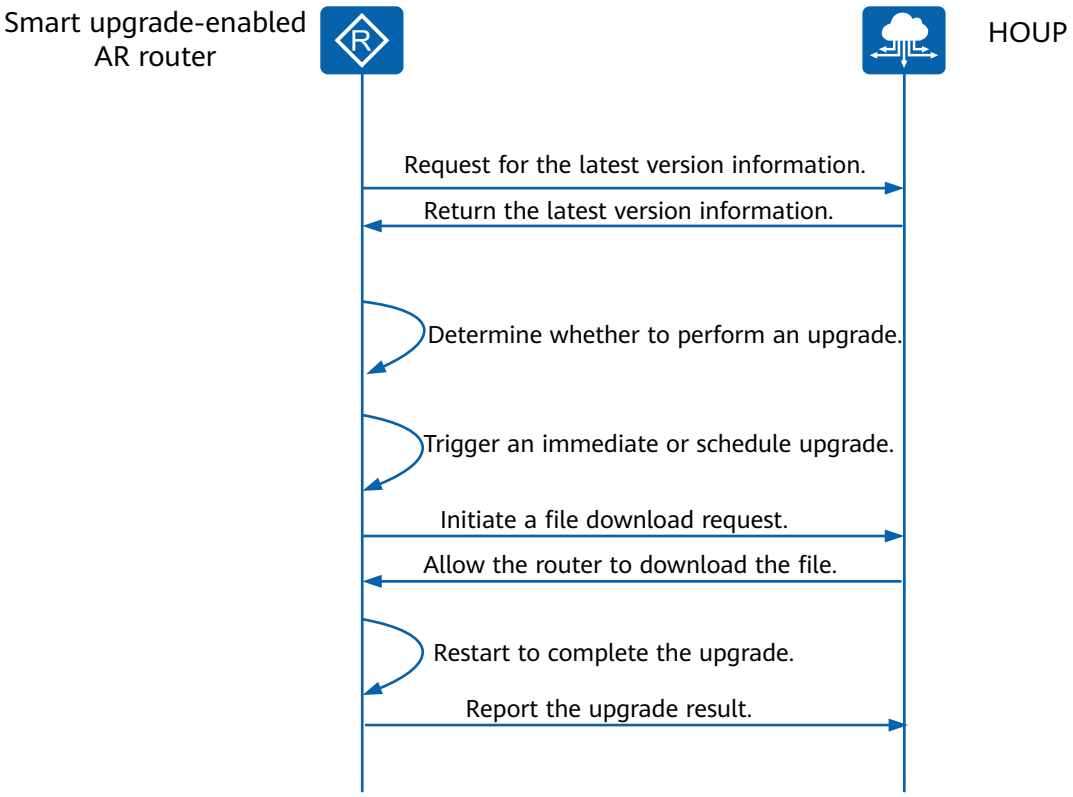


Smart Upgrade Procedure

Figure 16-2 shows the process in which a smart upgrade-enabled router exchanges with the HOUP.

 Copyright © Huawei Technologies Co., Ltd.

Figure 16-2 Smart upgrade procedure



The procedure is as follows:

1. The router reports its status information to the HOUP to request for the latest version information 10 minutes after the smart upgrade function is enabled.
2. After obtaining the status information, the HOUP returns the latest version information, including the latest system software version and patch information to the router based on a specified policy.
3. After the router obtains the latest version information, a user determines whether to upgrade the router according to the actual situation.
4. If the router needs to be upgraded, the user can further select the immediate or scheduled upgrade policy.
5. The router performs a smart upgrade and requests for the latest system file from the HOUP based on the upgrade policy selected by the user.
6. The HOUP responds to the download request of the router and transfers the system file to the router.
7. After obtaining the system file, the router automatically configures it as the file for next startup and restarts.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The router clears the original upgrade configuration in this procedure. During a restart, the router automatically saves and backs up configurations to the file named **vrpcfg_auto_backup.zip** or **vrpcfg_auto_backup.cfg**. Save the current configuration and export the configuration file in advance.

8. After the upgrade is completed, the router automatically reports the upgrade result to the HOUP. If the upgrade fails, the HOUP notifies maintenance engineers of the failure.

16.3 Licensing Requirements and Limitations for Smart Upgrade

Involved Network Elements

An AR router needs to cooperate with the HOUP to implement smart upgrade.

Licensing Requirements

Smart upgrade is a basic feature of an AR router and is not under license control.

Feature Limitations

- Only the AR100, AR120, AR150, AR160, AR200, and AR1200 series routers support this function.
- The router will restart during the upgrade, interrupting services.
- During smart upgrade, the router automatically saves the configuration information. To avoid unexpected configuration loss, you are advised to save the current configuration and export the configuration file in advance.

16.4 Configuring Smart Upgrade

Prerequisites

- An AR router resides on a public network and connects to the HOUP.
- There are reachable routes between Router and the DNS server.

Procedure

Step 1 Configure DNS.

1. Run **system-view**
   The system view is displayed.
2. Run **dns resolve**

   Dynamic domain name resolution is enabled.

   By default, dynamic DNS resolution is disabled.
3. Run **dns proxy enable**

 Copyright © Huawei Technologies Co., Ltd.

DNS Proxy is enabled.

By default, DNS proxy is disabled.

4. Run **dns server** *ip-address*

The IP address of the DNS server is configured.

By default, no IP address of the DNS server is configured.

Step 2 Load the HOUP certificate.

By default, the HOUP certificate is saved in default storage medium of the router without manual intervention (the certificates are **houp.huawei.com_local.cer** and **Actalis_CA.cer**). If the certificate expires, you can log in to the web page and upgrade the certificate on the **Intelligent Upgrade** page.

1. Run **pki realm** *realm-name*

A PKI realm is created and the PKI realm view is displayed.

By default, a PKI realm named **default** exists on a device. This realm can be modified, but cannot be deleted.

NOTE

In smart upgrade scenarios, the PKI realm name must be **defaultPki_houp**; otherwise, the device cannot connect to the HOUP.

2. Run **quit**

Return to the system view.

3. Run **pki import-certificate local realm** *realm-name* **pem filename** *filename*

A local certificate is imported to the specified PKI realm.

In this scenario, the PKI realm must be specified as **defaultPki_houp**, and the local certificate must be **houp.huawei.com_local.cer**.

4. Run **pki import-certificate ca realm** *realm-name* **pem filename** *filename*

A CA certificate is imported to the specified PKI realm.

In this scenario, the PKI realm must be specified as **defaultPki_houp**, and the CA certificate must be **Actalis_CA.cer**.

Step 3 Configure a client SSL policy.

1. Run **ssl policy** *policy-name* **type client**

A client SSL policy is created and the client SSL policy view is displayed.

2. Run **pki-realm** *realm-name*

A PKI realm is specified for the client SSL policy.

By default, no PKI is specified for the client SSL policy on the router.

In this scenario, the specified PKI realm must be **defaultPki_houp**.

3. Run **server-verify enable**

Certificate-based SSL server verification is enabled.

By default, certificate-based SSL server verification is enabled.

4. Run **quit**

Return to the system view.

 Copyright © Huawei Technologies Co., Ltd.

Step 4 Run **smart-upgrade enable**

Smart upgrade is enabled.

By default, smart upgrade is disabled.

Step 5 (Optional) Run **smart-upgrade information telephone** *telephonenum* **email** *emailaddress*

The contact number and email address for smart upgrade are set.

By default, no contact number or email address is set for smart upgrade.

NOTE

The contact number and email address are used only for emergency contact upon an upgrade failure.

Step 6 Run **quit**

Return to the user view.

Step 7 Run **display smart-upgrade information**

Details about smart upgrade are displayed.

Step 8 Run **system-view**

The system view is displayed.

Step 9 Configure smart upgrade.

When figuring out that there is a new system software version available for upgrade according to the **display smart-upgrade information** command output, you can configure an upgrade policy in either of the following methods:

- Run **smart-upgrade right-now**

  Smart upgrade is performed on the router immediately.
- Run **smart-upgrade time** *HH:MM:SS* { **weekly** | **monthly** | **yearly** }

  The scheduled smart upgrade policy is configured.

  By default, the start time or interval for scheduled smart upgrade is not set.

----End

Verifying the Upgrade

After the upgrade is completed, run the **display version** or **display patch-information** command to check the current version or patch information of the router.

16.5 Example for Configuring Smart Upgrade

When a large number of devices need to be upgraded to a recommended version, you can deploy the smart upgrade function to implement rapid upgrade of devices.

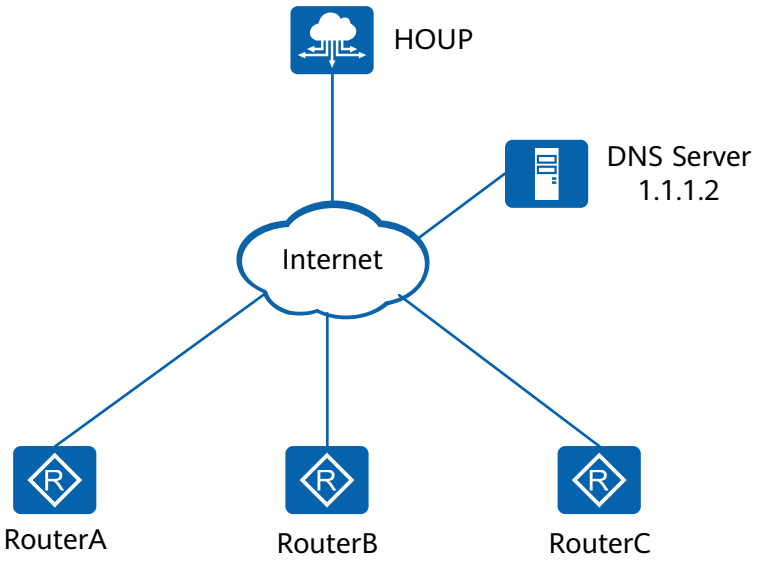
Networking Requirements

As shown in **Figure 16-3**, RouterA, RouterB, and RouterC reside on a public network and can communicate with the HOUP through the Internet. These routers

 Copyright © Huawei Technologies Co., Ltd.

have reachable routes to the DNS server. Certificates **houp.huawei.com_local.cer** and **Actalis_CA.cer** of the HOUP have been stored in the storage medium of the devices. The customer wants to deploy smart upgrade to implement online upgrade of the software or patch by connecting the devices to the HOUP.

Figure 16-3 Configuring smart upgrade



Configuration Procedure

The configuration of RouterB and RouterC is similar to that of RouterA, and is not mentioned here. The following uses RouterA as an example.

1. Configure DNS functions on RouterA, including the dynamic domain name resolution service.

```
<Huawei> system-view
[Huawei] dns resolve
[Huawei] dns proxy enable
[Huawei] dns server 1.1.1.2
```

2. Configure a PKI realm named **defaultPki_houp** on RouterA and import the certificates.

```
<Huawei> system-view
[Huawei] pki realm defaultPki_houp
[Huawei-pki-realm-defaultPki_houp] quit
[Huawei] pki import-certificate local realm defaultPki_houp pem filename
houp.huawei.com_local.cer
[Huawei] pki import-certificate ca realm defaultPki_houp pem filename Actalis_CA.cer
```

3. Configure an SSL policy on RouterA and bind the policy to the PKI realm named **defaultPki_houp**.

```
[Huawei] ssl policy defaultPolicy_houp type client
[Huawei-ssl-policy-defaultPolicy_houp] pki-realm defaultPki_houp
[Huawei-ssl-policy-defaultPolicy_houp] server-verify enable
[Huawei-ssl-policy-defaultPolicy_houp] quit
```

 Copyright © Huawei Technologies Co., Ltd.

4. Configure smart upgrade on RouterA.

```
[Huawei] smart-upgrade enable
[Huawei] smart-upgrade information telephone 123456789 email test@huawei.com
[Huawei] quit
```

5. Check smart upgrade details.

```
<Huawei> display smart-upgrade information
Info:Loading the information.Please wait for a few minutes.
Scheduled upgrade:              Enable
Next upgrade time:              2019-07-17 23:00:00

Check for new version:          Upgrade required
Recommended software version:  V200R010C00SPC600
Recommended patch version:      None
Upgrade description:
Firmware and Patch Description in English:1)description:2)description:

Info update time:               2019-07-11 14:17:06

Cancellation status:            Initial
Upgrade status:                 Initial
Software package size(B):       155945856
Patch package size(B):          0
Download progress(%):           0
Download speed(KB/s):           0.00
Download status:                notStart
Software package name:          AR120-V200R010C00SPC600.cc
Patch package name:             None
Patch type:                     None
Last upgrade type:              now
Last upgrade time:              2019-06-29 15:49
Last upgrade result:            None

Device name:                    AR129CGVW-L
ESN:                            21500102152SF5900070
SoftWare version:               V200R010C00SPC200
Patch version:                  None

Last startup software::         flash:/ar120_spc200.cc
Last startup patch:             None
Backup configuration file:      vrpcfg_auto_backup.zip
Last startup voice package:     None
Last startup license:           None
```

The message "Check for new version: Upgrade required" is displayed in the command output, indicating that a new software version is available for upgrade.

6. Perform smart upgrade immediately.

```
<Huawei> system-view
[Huawei] smart-upgrade right-now
Info: Connecting to the smart upgrade platform...Please wait for a few minutes.
Info: Starting to download file AR120-V200R010C00SPC600.cc
100%
Info: Downloading file AR120-V200R010C00SPC600.cc succeeded.
smart-upgrade: 155944876 byte(s) received in 433 second(s) 355.71Kbyte(s)/sec.
Info: Starting to download file AR120-V200R010C00SPC600.cc.asc
Info: Verifying the system software package using the signature file .....................
.........
Info: Verification succeeded.
Info: The device needs to be reboot to proceed with the upgrade. Continue? (Y will be selected by default 30 seconds later)(Y/N)[Y]:Y
```

After a restart, the device is upgraded to the new version.

Verifying the Upgrade

Check the software version after the upgrade.

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.170 (AR120 V200R010C00SPC600)
Copyright (C) 2011-2018 HUAWEI TECH CO., LTD
Huawei AR129CGVW-L Router uptime is 2 weeks, 6 days, 20 hours, 11 minutes

MPU 0(Master) : uptime is 2 weeks, 6 days, 20 hours, 10 minutes
SDRAM Memory Size    : 512      M bytes
Flash 0 Memory Size  : 512      M bytes
USB Disk0 Memory Size: 12       M bytes
MPU version information :
1. PCB       Version  : AR129CGVW-L VER.C
2. MAB       Version  : 0
3. Board     Type     : AR129CGVW-L
4. BootROM   Version  : 1
```